A COMPREHENSIVE APPROACH TO THIRD PARTY RISK MANAGEMENT

WHITE PAPER

What's The Purpose Of Third Party Risk Management?

Your company deploys advanced IT security controls and follows best practices to prevent unauthorised access to your systems and protect sensitive company and customer data. Unfortunately, it's not enough.

It's not enough because there is an entire spectrum of risks you don't directly control – access to your systems and sensitive data by your suppliers. Simply stated: the overall security of your data and systems is dependent on the risk controls provided by your suppliers.

A recent Vulnerability Index research report released by Privileged Identity Management company Bomgar, showed that breaches occurring from third parties account for two-thirds of the total number of reported breaches[1]. In addition, the study found that:

89 suppliers

on average, are accessing a company's network every week

Only **46%**

of companies said they know the number of log-ins that could be attributed to suppliers

Less than **51%**

enforce policies around Third Party access

69%

said they definitely or possibly suffered a security breach resulting from supplier access in the past year

Studies like this and many others over the past few years have driven the consensus among security professionals that the risk posed by third parties is not only substantial, but it is increasing, and there is no "one size fits all" solution to the problem.

This is why you need a comprehensive approach to your Third Party Risk Management (TPRM) program that allows you to:

Identify the security controls a supplier must have based on the services they provide

Determine if they are maintaining those controls

Develop plans for corrective action to be taken by the supplier

Monitor the supplier's threat environment for additional external risks and operational issues

Reduce collection time by leveraging shared, standardised risk information collected for other companies who utilise the same supplier

[1] Bomgar. Vendor Vulnerability Index brings security risk of third-parties to light, April 2016

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk

Why is Third Party Risk Management So Complicated?

TPRM is a growing concern for the CISO, CIO, CEO, and even Board-level stakeholders. In fact, Gartner recently stated in their June 2017 Magic Quadrant for IT Vendor Risk Management that by 2020, 75% of Fortune Global 500 companies will treat supplier risk management as a board-level initiative to mitigate brand and reputation risk[2].

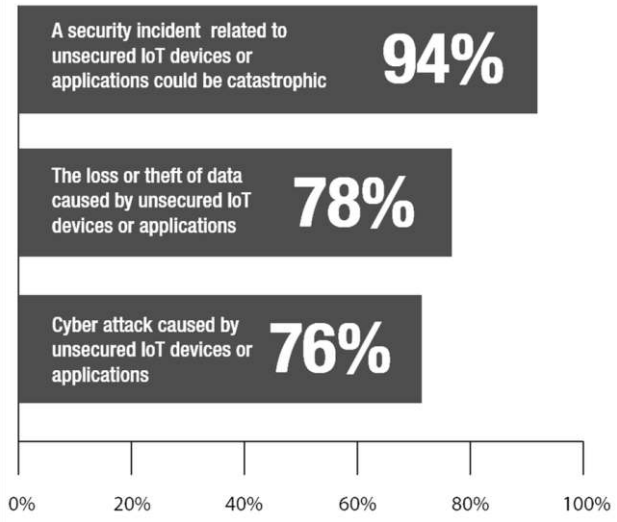
In addition, with the introduction of the Internet of Things (IoT), organisations are quickly realising that they are not prepared, and according to a recent Poneman and Shared Assessments study, are still "relying on technologies and governance practices that have not evolved to address emergent IoT threat vectors." Even though 25% of respondents in this study stated that their board of directors require assurances that IoT risk among third parties is being assessed, managed, and monitored appropriately, only 27% said they have the resources to support it[3].

The reality is that once your data is under the control of your suppliers, it's still YOUR data. It is up to you to ensure your suppliers have adequate security controls in place and that they keep those controls current based on the ongoing changes to the threat environment. Further complicating this, are many supplier variables that you need to consider, such as:

- Whether the supplier has custody of, or access to, your sensitive information
- Whether the supplier has access to your company's network
- Size of the supplier
- Location of the supplier
- Sophistication of the supplier's IT and security teams
- If the supplier itself outsources services
- The supplier's product or service
- Regulations

IoT risks in the next two years

Very likely, somewhat likely & likely responses combined



Other factors to consider include geography, recent events relating to the supplier (e.g. a data breach, bankruptcy filing, lawsuit, leadership change), and any number of other variables unique to the millions of suppliers in business globally.

What does this supplier relationship complexity mean for security professionals responsible for third party risk management? In short, they need several tools to efficiently gain visibility into and manage the risk of their supplier ecosystem.

2 Gartner. Magic Quadrant for IT Vendor Risk Management, June 2017

3 Poneman Institute. The Internet of Things (IoT): A New Era of Third-Party Risk, May 2017

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk

One Size Doesn't Fit All

Supplier assessment must be 'fine-tuned' to the type of data involved, the systems being accessed, and the nature of the services provided by the supplier. For example, would you ask a 15-person law firm that handles your patent filings and litigation to complete the same comprehensive questionnaire they send to a cloud-based application provider? Would a healthcare company ask their laboratory analysis suppliers the same set of risk questions they would their payroll company? How much do you really care about the security controls of the supplier that landscapes your company grounds? Software Development Life Cycle (SDLC) processes are obviously important for suppliers delivering applications embedded in your organisation's operations, but they're irrelevant to a claims processing supplier of a car insurance company.

Once the proper scope is established, assessment due diligence must be requested from the supplier, validated, and then analysed. Upon completion, decisions are then made about risk acceptance and/or mitigation. Results must be consolidated and reports generated to senior management that define outsourcing risk and the operational efficiency of the TPRM process. This effort - extended over dozens, hundreds, or even thousands of suppliers - is essentially impossible to conduct without software automation.

Third Party Assessment Software

Assessment (upper case "A") has become the go-to word in the third party risk world, but whether a formal Assessment is appropriate for a supplier or not, the requirement to assess (evaluate, appraise, gauge, estimate, determine, etc.) the risk of the supplier doesn't go away. Multiple options are needed to have a successful TPRM program.

Fortunately, technology is evolving to provide exactly such options for the growing third party risk community. First, automated Assessment tools are significantly more sophisticated than their predecessor generations. Today's Third Party risk management software offers the kinds of features that enable supplier content tuning, including:

- ✓ Ability to "tier" suppliers, or determine which surveys and other requests to make of suppliers based on their relationship to the organisation
- ✓ Ability to pull completed and reviewed standard content from supplier evidence networks, saving both the suppliers and your organisation countless hours of time
- ✓ Ability to build custom, supplemental surveys that address the gaps in standard content
- ✓ Risk score flexibility to enable users to customise to their risk needs within the tools
- ✓ Shipping with off-the-shelf, industry-accepted standard content
- ✓ Built-in workflows that provide automated and auditable interaction with suppliers to facilitate remediation and/or provide greater risk visibility into your supplier ecosystem

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk

Continuous Threat Monitoring

Unlike first generation continuous monitoring offerings, contemporary services provide a holistic view of supplier risk as determined by external events and internal security posture. Rather than focusing exclusively on outdated measures of security provided by external network scans, today's monitoring products gather risk event data from several sources on an on-going basis to form a risk picture across the supplier's entire spectrum of potential threats to your organisation.

Data breaches are just one way in which your relationship with a supplier can negatively impact your operations and external network scans provide little insight into a supplier's vulnerability in today's sophisticated threat environment. Financial risk events, operational challenges (such as natural disasters or leadership shake-ups), regulatory citations, fraudulent practice claims, and lawsuits are just a few examples of the kinds of events that can greatly impact the risk of a supplier to your organisation. Fortunately, options exist in advanced TPRM solutions for third party risk professionals to keep track of their suppliers on a daily basis, beyond the narrow focus of first-generation monitoring tools with a narrow-minded view of risk.

Small Business Supplier Inspection

One of the challenges that has traditionally faced the third party risk community is the inability to gauge the risk of small suppliers, those with only 2 to 100 employees. Compounding the challenge is the increasing importance of these small suppliers to the operations of many organisations and their resulting exposure to sensitive data. Small law firms, local printing companies, production studios, small PR organisations, or family-run claims processing companies are just a few examples of suppliers who can comprise a small number of employees, but require access to a large organisation's sensitive information.

The risk associated with this segment of suppliers continues to grow as they increasingly become targets for hackers. Lacking the resources and skill sets of larger organisations, criminals rightfully identify them as easier targets than their customers. According to a recent Symantec study almost one-half of all cyber-attacks (43%) last year were against small businesses[4] with a 2017 Webroot Cyber Threat report finding that IT decision makers at 96% of SMBs in the US, UK, and Australia believe their organisations will be susceptible to external cybersecurity threats this year[5].

Until recently, evaluating the risk of these small suppliers has been an elusive goal. However, with advanced TPRM solutions, automated inspection and risk evaluation solutions are available to benefit both the small supplier, as well as their large and medium size customers. Low-footprint agents gather information on the endpoint security state of a small supplier, process the information, and generate security deficiency reports. In addition, recommendations are made for the supplier to improve their security profile. Your organisation now has a means to assess and help mitigate the risk of very small, essential suppliers, and the suppliers – often too small to employ IT resources, let alone security professionals – have a tool to help them improve their security and keep your sensitive data safe.

4 Symantec. Internet Security Threat Report, 2017
5 Webroot. Cyber Threat to Small – and Medium-Sized Businesses in 2017, 2017

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk

Evidence Sharing Networks

A relatively new innovation in third party risk is providing third party risk managers with all of the benefits of the traditional Assessment process, but with much less aggravation. The advent of Supplier Evidence Sharing Networks is making completed, verified, standard surveys available to organisations while eliminating the tedious time-and-resource consuming process of collecting accurate data from suppliers.

The “Complete-Once, Share-Many” model of supplier sharing networks means the burden on suppliers is similarly alleviated. By greatly reducing the effort required to collect or complete surveys, it means that both first and third parties can spend much less time gathering controls data and much more time on what’s important: working together to decrease control gaps and reduce overall risk.

Evidence network sharing is a feature built into advanced supplier risk management software, so that users can not only leverage advanced workflows, reporting, scoring, and other features of these enterprise software solutions, but can also augment that rich functionality with “off-the-shelf” supplier evidence that can instantly form the foundation of a comprehensive and effective third party risk management program.

Mixing and Matching Capabilities to Meet Your Program Needs Today and Tomorrow

Very rarely will only one of the four solutions discussed in this whitepaper satisfy the TPRM needs of an organisation with such diverse suppliers - and that’s exactly the point. Having the access to all four components is necessary to build a highly-functioning, efficient third party risk program - and Prevalent is the only solution provider in the market today that can deliver all four advanced solutions. Prevalent developed the first purpose-built Third Party Risk Management cloud-based platform in 2012 and is the only company that offers a complete, integrated suite of solutions that includes automated assessment software, continuous threat monitoring, leading-edge SMB inspection, and innovative supplier evidence sharing networks.

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk

About DVV Solutions

DVV Solutions was established in 1999, and has become one of the UK's leading providers in the design, implementation and management of Third Party Risk Management (TPRM) and IT Security services.

We have a proven model for Third Party risk reduction and mitigation. Our suite of consultative and managed services improve your ability to manage increasing numbers and complexity of outsourced supplier risk backed by leading risk intelligence and automation platforms.

Our ethos is to provide you the best value for money by offering the highest quality of service within a clear and consistent cost model. We do this by leveraging our extensive experience in the IT services sector and our best-of-breed technology and service partners.

As a Shared Assessments program member and registered Assessment Firm we utilise industry-standard practices including Standardised Information Gathering (SIG) questionnaires and Agreed Upon Procedures (AUP) for onsite assessments.

Our channel partnership agreement with Prevalent Inc. enables DVV Solutions to deliver and support Prevalent technologies to UK and European customers and add significant value to their Third Party Risk Assessment capabilities. Recently named a Leader in the Gartner Magic Quadrant for IT Supplier Risk Management, Prevalent helps global organisations manage and monitor the security threats and risks associated with Third and Fourth Party suppliers.

DVV solutions

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

Tel: +44 (0) 161 476 8700
Email: enquiries@dvvs.co.uk
Web: www.dvvs.co.uk