May 2018

CyberGRX

Collaborative Accountability in Third Party Cyber Risk Management

SOLUTION***PERSPECTIVE***

Governance, Risk Management & Compliance Insight

Table of Contents

TALK TO US . . .

We look forward to hearing from you and learning what you think about GRC 20/20 research. GRC 20/20 is eager to answer inquiries from organizations looking to improve GRC related processes and utilize technology to drive GRC efficiency, effectiveness, and agility.

CyberGRX

Collaborative Accountability in Third Party Cyber Risk Management

Increasing Exposure to Cyber Risk in Third-Party Relationships

Brick and mortar business is a thing of the past: physical buildings and conventional employees no longer define an organization. The modern organization is an interconnected mesh of relationships, interactions, and transactions that span traditional business boundaries. Over half of an organization's 'insiders' are no longer traditional employees. Insiders now include suppliers, vendors, outsourcers, service providers, contractors, subcontractors, consultants, temporary workers, agents, brokers, dealers, intermediaries, and more. Over sixty-percent of data breaches are linked to a third party and not from inside the traditional organization. The people not on the company's payroll and the infrastructure that the company doesn't control may pose the biggest risk. Complexity grows as these interconnected relationships, processes, and systems nest themselves in layers of subcontracting and supplier relationships.

In this context, organizations struggle to adequately govern information security risk in third-party business relationships. Risk and compliance challenges do not stop at traditional organizational boundaries as organizations bear the responsibility of the actions or inactions of their extended third party relationships. An organization can face reputational and economic disaster by establishing or maintaining the wrong business relationships, or by allowing good business relationships to sour because of poor information security governance and risk management. When questions of security arise, the organization is held accountable, and it must ensure that third parties behave appropriately.

The challenge: Can you attest to the information security governance, risk management, and compliance for third parties across your organization's business relationships?

Governing third party relationships, particularly in context of information security risk and compliance, is like the hydra in mythology: organizations combat each head, only to find more heads springing up to threaten them. Departments are reacting to third party management in silos and the organization fails to actively implement a coordinated strategy for third party management across the enterprise. Organizations manage third parties differently across different departments and functions with manual approaches involving thousands of documents, spreadsheets, and emails. Worse, they focus their efforts at the formation of a third party relationship during the on-boarding process and fail to govern risk and compliance throughout the lifecycle of the relationship.

This fragmented approach to third party governance brings the organization to inevitable failure. Reactive, document-centric, and manual processes cost too much and fail to

actively govern, manage risk, and assure compliance throughout the lifecycle of a third party relationship. Silos leave the organization blind to the intricate exposure of risk and compliance that do not get aggregated and evaluated in context of the organization's goals, objectives, and performance expectations in the relationship.

Failure in third party management happens when organizations have:

- **Growing risk and regulatory concerns with inadequate resources.** Organizations are facing a barrage of growing regulatory requirements and expanding risks around the world. Many target third party relationships specifically, while others require compliance without specifically addressing the context of third parties. Organizations are encumbered with inadequate resources to monitor risk and regulations impacting third party relationships and often react to similar requirements without collaborating with other departments, which increases redundancy and inefficiency.

- **Interconnected third party risks that are not visible.** The organization's risk exposure across third party relationships is growing increasingly interconnected. An exposure in one area may seem minor but when factored into other exposures in the same relationship (or others) the result can be significant. Organizations often lack an integrated and thorough understanding of the interconnectedness of performance, risk management, and compliance of third parties.

- **Silos of third party oversight.** Allowing different departments to go about third party management without coordination, collaboration, consistent processes, information, and approach leads to inefficiency, ineffectiveness, and lack of agility. This is exacerbated when organizations fail to define responsibilities for third party oversight and the organization breeds an anarchy approach to third party management leading to the unfortunate situation of the organization having no end-to-end visibility and governance of third party relationships.

- **Document, spreadsheet, and email centric approaches.** When organizations govern third party relationships in a maze of documents, spreadsheets, and emails it is easy for things to get overlooked and buried in mountains of data that are difficult to maintain, aggregate, and report on. There is no single source-of-truth on the relationship and it becomes difficult, if not impossible, to get a comprehensive, accurate, and current-state analysis of a third party. This manual document-centric approach requires a tremendous amount of staff time and resources to consolidate information, analyze, and report on third party information. When things go wrong, audit trails are non-existent or are easily covered up and manipulated as they lack a robust system of record of who did what, when, how, and why.

- **Scattered and non-integrated technologies.** When different parts of the organization use different approaches for on-boarding and managing third parties, the organization can never see the big picture. This leads to a significant

amount of redundancy and encumbers the organization when it needs to be agile.

- **Due diligence done haphazardly or only during on-boarding.** Risk and compliance issues identified through an initial due diligence process are often only analyzed during the on-boarding process to validate third parties. This approach fails to recognize that additional risk and compliance exposure is incurred over the life of the third party relationship and that due diligence needs to be conducted on a continual basis.

- **Inadequate processes to monitor changing relationships.** Organizations are in a constant state of flux. Governing third party relationships is cumbersome in the context of constantly changing regulations, risks, processes, relationships, employees, suppliers, strategy, and more. The organization must monitor the span of regulatory, geo-political, commodity, economic, and operational risks across the globe in context of its third party relationships. Just as much as the organization itself is changing, each of the organization's third parties is changing introducing further risk exposure.

- **Third party performance evaluations that neglect risk and compliance.** Metrics and measurements of third parties often fail to properly encompass risk and compliance indicators. Too often metrics from service level agreements (SLAs) focus on delivery of products and services by the third party but do not include monitoring of risks, particularly compliance and ethical considerations.

The bottom line: When the organization approaches information security in third party management in manual processes, there is no possibility to be intelligent about information security governance, risk management, and compliance in these relationships. An ad hoc approach to third party management results in poor visibility across the organization, because there is no framework or architecture for managing third party information security risk and compliance as an integrated framework. It is time for organizations to step back and define a strategy and process to govern risk in third party relationships that is supported and automated with services and technology that enable collaborative accountability between the organization and it's third parties.

CyberGRX

Collaborative Accountability in Third Party Cyber Risk Management

CyberGRX is a third-party cyber risk management solution provider that GRC 20/20 has researched, evaluated, and reviewed that is agile for use in complex, distributed, and dynamic business environments to manage an organization's third party management processes in context of cyber security. CyberGRX delivers a new breed of integrated and collaborative services and technology that leverages an intuitive exchange network platform to streamline third party management to make it more efficient, effective, and agile. The solution delivers significant business value and brings a contextual understanding of information security risk in third party management across an organization's distributed and heterogeneous extended enterprise environment.

CyberGRX is privately held and was founded in 2015. Over the past 3 years, it has developed an integrated service, network exchange, and technology to streamline third party management. Their focus is to address the issue of inefficiency when a third party is being assessed by not one, but thousands of other organizations. Not only is this manual process inefficient, but also ineffective and inagile as these assessments were highly redundant and time consuming, slowing these organizations down – both the organization itself as well as the third parties it works with. To address this, CyberGRX was founded to create a third party global cyber risk management exchange.

GRC 20/20's evaluation, research, and interactions with CyberGRX clients has determined the following:

- **Before CyberGRX:** Clients of CyberGRX typically are replacing manual processes that are encumbered by static data found in documents, spreadsheets, and emails or siloed third party management solutions that do not address the collaboration and network exchange needs of multiple organizations assessing third parties. Such approaches can be very manual, time-consuming, and prone to errors, particularly in aggregation and reporting on data that involves hundreds to thousands of documents and spreadsheets. Organizations found they ran an ad hoc third party risk program that barely kept up with new third parties because of manual processes. They were swamped with new third parties, and had a range of legacy third parties that they could not begin to think of going back to provide assurance on. This resulted in lots of legacy third parties that never had a security review. These organizations had to either add FTEs to address the risk exposure in third party relationships or look for a solution that helped automate and collaborate with third parties more efficiently, effectively, and in a way that is agile.

- **Why CyberGRX:** Organizations choose CyberGRX as they are looking for a single integrated information service for third party cyber risk management to replace manual processes encumbered with documents, spreadsheets, and emails. They are looking for a single collaborative process that can handle a complex array of third parties that can be assessed once and provide assurance to many relationships on a continuous basis. Other solutions these clients looked at could not scale the way they needed it to. The main reasons why clients select CyberGRX is:

  - *Faster assessment and continuous monitoring* of third party relationships where organizations and their third parties participate in a shared network exchange of information to promote collaborative accountability and ongoing insight.

  - *Replacement of static, once a year assessment processes* that often comes with a shared spreadsheet. Their standardized assessment process collects structured data which lives on the Exchange. Once a third party completes an assessment, they can easily update their data on the Exchange - and share that data/assessment with as many third parties as they like.

- *Increase insight through dynamic data* that comes from having a structured and standardized assessment approach. This data lives on the Exchange, not in a spreadsheet. It can be easily updated by third parties and enterprises can easily run analytics across it. Enterprises get the data in an actionable format with advanced analytics so they can easily deduce insights from it - and prioritize their resources accordingly.

- *Scale assessment activity* to a level that's commensurate with their exposure. Organizations need to be able to assess and monitor more third parties, but lack the resources to do so. CyberGRX gives those organizations the extra hands they need to cover more of their ecosystem.

- How CyberGRX is used: As a new breed of GRC third party risk solution that integrates technology and services for collaborative accountability in these relationships. Organizations are particularly pleased that they can finally address the assessment of both new as well as existing legacy third parties they could not get back to before. Some organizations find value in CyberGRX as they sit on both sides, they need to assess their own third party relationships, but also find they are a third party to many other organizations and there is value in providing a common assessment that is good for multiple relationships and requests they have to respond to from organizations who request security attestations, self-assessments, and onsite/remote audits.

- Where CyberGRX has excelled: Organizations consistently state that CyberGRX has improved the quality of their third party related information and their ability to report on risks. This improves the organization's overall visibility into third party risk exposure while eliminating the overhead of managing manual processes encumbered by hundreds to thousands of spreadsheets, documents, and emails. Clients find that the solution and exchange network is flexible to adapt to their organization's needs and provides them the ability to grow and mature their program over time. Overall, users find the solution intuitive and easy to use, fast to deploy, and agile to meet diverse organization and process requirements. They particularly find that the hands off process is of value when they identify a vendor and send it to CyberGRX for assessment the process is then outsourced.

What CyberGRX Does

GRC 20/20 has evaluated the features and capabilities of the CyberGRX solution and finds that it delivers an agile, intuitive, and engaging solution for information security governance in third party management. CyberGRX is an intuitive integrated service and platform that modernizes how organizations work and interact with third party management processes and share information with other organizations. It is used to collect, organize, link, report, and analyze third party information security data with increased control, transparency, and collaborative accountability between an organization and it's third parties.

The intriguing point about CyberGRX is that it provides significant benefits to both sides of the relationship. The CyberGRX Global Risk Exchange and Risk Assessments-as-a-

service approach makes the process of third party management more efficient, effective, and agile for the organization as well as the third party.

Some specific features and capabilities of CyberGRX include:

- **Global Risk Exchange.** The heart of CyberGRX is a community network that provides an exchange delivery model that builds a community and collaboration. Organizations and third parties participate in the Exchange to do a common assessment that is good for many relationships.

- **Dynamic & actionable dashboards.** CyberGRX provides 360° contextual visibility and intelligence into an organization's ecosystem of third party relationships to identify the riskiest third parties while prioritizing remediation efforts with the most yield. Third party data lives in the Global Risk Exchange and is updated with mitigation efforts and as threat levels change – this is more agile than the static view an annual shared assessment provides.

- **Analytics.** This provides actionable insight that integrates industry threat data, a rules engine and outside-in validation. Enabled by structured assessment data, CyberGRX analytics provide actionable insights that integrate data from organizations and their third parties so they can prioritize and mitigate risk CyberGRX analytics also provides immediate pre-assessment insights into third party risk business exposure - the potential likelihood and impact that a third party cyber event would have on your business

- **Standards-based.** CyberGRX third party risk assessments are based on NIST 800-53 with an information architecture that maps to other significant and common regulations and standards.

- **Shared cost.** The CyberGRX Global Risk Exchange shares the cost of effective third party management between organizations and third parties in a shared pricing model.

- **Risk assessments as a managed service.** The backbone of the Global Risk Exchange is the standardized and structured third-party risk assessments that identify and prioritize risk. CyberGRX assessments are configurable and intuitive and allow skip level logic so that third parties do not need to respond to questions that are not relevant to them. Assessments include self-validation and verification. They are scalable to degrees of assessment depth and appropriately corresponding levels of validation, which includes:

    - *High-risk third party assessments.* This is their most comprehensive assessment which includes a long form questionnaire that is completed by the third party, that is then followed by an onsite evidence to validate control maturity and effectiveness of the third party.

- ***Medium-risk third party assessments.*** This is their assessment for medium risk third parties which includes an abbreviated form questionnaire that is completed by the third party, followed by automated validation through a rules engine based on proprietary algorithms to identify inconsistencies in assessment responses.

- ***Low-risk third party assessments.*** This is their assessment for low-risk third parties which includes an abbreviated short form questionnaire that is completed by the third party followed by self-attestation to the answers.

There are two sides to the CyberGRX interaction, the organization trying to manage it's third party relationships and the third party responding to information requests and due diligence from these organizations. As organizations operate in an interconnected mesh, it is common for an organization to be part of both sides of this community.

The benefits to the enterprise organization (the one trying to manage third party risk) is a streamlined process, where assessments are managed as a service, and actionable, structured data is made available through the Exchange – providing them with ongoing/current insight into potential risks and where to focus their efforts. The process and approach for organizations utilizing CyberGRX to manage it's third party relationships is as follows:

1. ***Upload*** third parties into the CyberGRX platform

2. ***Answer*** preliminary questions to determine inherent risk of third party scope and relationships

3. ***Understand*** business exposure through visualizations on business relationships and risk so the organization can prioritize it's assessment strategy

4. ***Order*** the appropriate tier of assessment (see above) to be done on each third party

5. ***Receive*** the CyberGRX report and risk mitigation strategy on third parties

6. ***Utilize*** CyberGRX to track remediation projects to completion

7. ***Monitor*** for changes to the organization's third party ecosystem on a continuous basis

From the third party perspective, shared spreadsheets are eating up your valuable resources and providing limited value. CyberGRX assessments use a smart, skip level logic approach, so they automatically calibrate responses—removing any redundant or irrelevant questions. And, once an assessment is complete, an organization can use The CyberGRX Exchange to proactively share it with any upstream partner they choose. Complete one assessment, share with many. The process and approach for third parties

responding to information requests and due diligence on the CyberGRX platform is as follows:

1. ***Complete*** a Tier 1, 2, or 3 CyberGRX Assessment as required by the organization you are partnering with

2. ***Receive*** a detailed roadmap for improving the security and control of your organization in context of this relationship

3. ***Implement*** CyberGRX's remediation strategies

4. ***Share*** the assessment with other upstream business partners and relationships

Benefits Organizations Have Received with CyberGRX

GRC is an integrated capability to reliably achieve objectives [GOVERNANCE], while addressing uncertainty [RISK MANAGEMENT], and acting with integrity [COMPLIANCE].[1] Successful GRC strategies deliver the ability to effectively mitigate risk, meet requirements, satisfy auditors, achieve human and financial efficiency, and meet the demands of a changing business environment. GRC solutions should achieve stronger processes that utilize accurate and reliable information. This enables a better performing, less costly, and more flexible business environment.

GRC 20/20 measures the value of GRC initiatives around the elements of efficiency, effectiveness, and agility. Organizations looking to achieve GRC value will find that the results are:

- **GRC Efficiency.** GRC provides efficiency and savings in human and financial capital resources by reduction in operational costs through automating processes, particularly those that take a lot of time consolidating and reconciling information in order to manage and mitigate risk and meet compliance requirements. GRC achieves efficiency when there is a measurable reduction in human and financial capital resources needed to address GRC in the context of business operations.

- **GRC Effectiveness.** GRC achieves effectiveness in risk, control, compliance, IT, audit, and other GRC processes. This is delivered through greater assurance of the design and operational effectiveness of GRC processes to mitigate risk, protect integrity of the organization, and meet regulatory requirements. GRC effectiveness is validated when business processes are operating within the

1 *This is the official definition of GRC found in the GRC Capability Model and other work by OCEG at www.OCEG.org.*

controls and policies set by the organization and provide greater reliability of information to auditors and regulators.

- **GRC Agility.** GRC delivers business agility when organizations can rapidly respond to changes in the internal business environment (e.g. employees, business relationships, operational risks, mergers, and acquisitions) as well as the external environment (e.g. external risks, industry developments, market and economic factors, and changing laws and regulations). GRC achieves agility when organizations can identify and react quickly to issues, failures, non-compliance, and adverse events in a timely manner so that action can be taken to contain these and keep them from growing.

In today's enterprises, the board of directors, the CEO and the CISO are increasingly concerned about unidentified cyber security risk from third parties. They are demanding that IT Risk teams manage the information security risk of increasing number of third party relationships. Third party Information security assessments are performed by costly and scarce SME's who typically use spreadsheets in a cumbersome and inherently non-scalable manual process. With regulators and CISO's demanding that more and more third party relationships be assessed, an enterprise-grade solution is an absolute requirement.

The CyberGRX service and solution enables organizations to manage cyber security risks from a fast-growing population of third party relationships, and to deliver the reporting to their CISO's, CEO's, and boards of directors are demanding. Some specific benefits organizations using CyberGRX have received, that GRC 20/20 has researched and interviewed, are:

- *Faster assessment* that enables organizations to assess as much as five times the third parties in one-third less the time.
- *Contextual risk awareness* that enables the organization to know which third parties pose the most risk to your enterprise.
- *Shift internal resources* from data reconcilers and compilers to risk managers.
- *Effectively mitigate risk* through a prioritized risk-based mitigation strategy.
- *Share costs* from crowd-sourced mitigation efforts in the CyberGRX Global Risk Exchange
- *Identify and understand* the remediation with the most return to the organization in reduced risk exposure.
- *Share a risk assessment* with multiple upstream partners to reduce assessment fatigue.

- *Increase assessments,* where one client stated they did sixty third party assessments last year and this year they are doing 200 assessments which is a 3-4x scale without adding headcount to their team.

- *Automation of enterprise-wide management* of third party cyber security risk that has generally been performed manually.

- *Reduction in errors* by allowing third parties to enter data directly into the system instead of emailing documents and information to the organization that were incomplete or incorrectly entered.

- *Significant efficiencies in time* through automation of workflow and tasks as well as reporting. Specifically, the time it took to build reports from hundreds to thousands of documents and spreadsheets now is just a matter of seconds.

- *Consistency and accuracy of information* as all internal stakeholders and third parties must conform to consistent processes and information collection. A single solution with a uniformed and integrated process and information architecture.

- *Accountability with full audit trails* of who did what and when; this particularly has delivered value in less things slipping through the cracks.

- *Notification and tasks that get done* results in less frustration, as well as overcoming frustration because things were not filled out and had to be sent back to a third party.

- *Greater visibility into third party information security risks* as all information is stored in one common data architecture which provides a single source of truth which is more accurate and readily available.

Considerations in Context of CyberGRX

Every solution has its strengths and weaknesses, and may not be the ideal fit for all organizations in all situations. While GRC 20/20 has identified many positive attributes of CyberGRX to enable organizations to achieve consistent third party management processes, readers should not see this as a complete and unquestionable endorsement of CyberGRX.

CyberGRX is improving the assessment experience for both the organization and its third parties. This is in contrast to many solutions in the market whose built-in capabilities do not lend to an assessment sharing and exchange approach, and the effort to implement these platforms is costly, often running into the millions of dollars and over a year to deploy.

Organizations using CyberGRX report that they love the ability to scale the number of third parties that are assessed with a more comprehensive assessment without adding headcount. Areas where clients would like to see the solution expand its capabilities would be in more robust features to provide more data beyond assessment of controls.

About GRC 20/20 Research, LLC

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis. We provide objective insight into GRC market dynamics; technology trends; competitive landscape; market sizing; expenditure priorities; and mergers and acquisitions. GRC 20/20 advises the entire ecosystem of GRC solution buyers, professional service firms, and solution providers. Our research clarity is delivered through analysts with real-world expertise, independence, creativity, and objectivity that understand GRC challenges and how to solve them practically and not just theoretically. Our clients include Fortune 1000 companies, major professional service firms, and the breadth of GRC solution providers.

Research Methodology

GRC 20/20 research reports are written by experienced analysts with experience selecting and implementing GRC solutions. GRC 20/20 evaluates all GRC solution providers using consistent and objective criteria, regardless of whether or not they are a GRC 20/20 client. The findings and analysis in GRC 20/20 research reports reflect analyst experience, opinions, research into market trends, participants, expenditure patterns, and best practices. Research facts and representations are verified with client references to validate accuracy. GRC solution providers are given the opportunity to correct factual errors, but cannot influence GRC 20/20 opinion.

GRC 20/20 Research, LLC
4948 Bayfield Drive
Waterford, WI 53185 USA
+1.888.365.4560
info@GRC2020.com
www.GRC2020.com