Cyber GRX

Cutting through the noise of third-party assessments

How CyberGRX Predictive Risk Profiles can provide actionable insights

Introduction

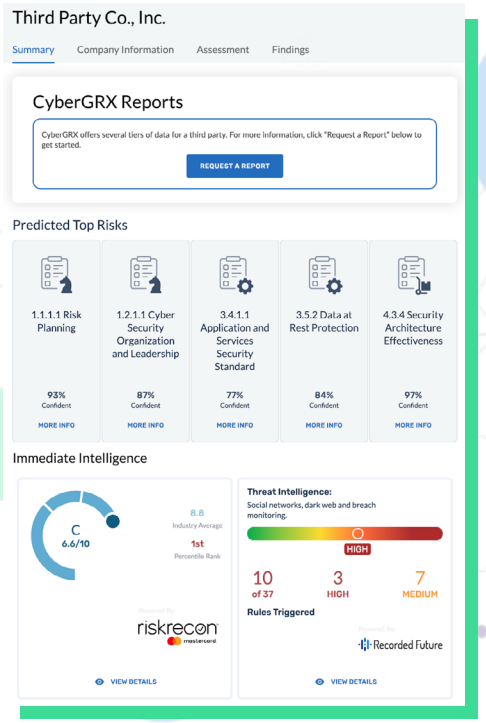
Third-party cyber risk management programs come in many varieties. Some struggle to get the data they need and others may be drowning in data. When using the traditional approach of collecting third-party assessments from each vendor within a business ecosystem, data can pile up and often be unactionable due to its collection in static spreadsheets or the fact that there are multiple assessment types that cannot be analyzed easily.

Just as threat intelligence provides useful information that can be applied to combat threats and better assess and improve an organization's security posture, Cyber Risk Intelligence can provide a similar set of actionable insights. Cyber Risk Intelligence is a new concept and is defined as the practice of collecting, standardizing, and analyzing data in reference to third-party security practices and technology infrastructure, and the use of that information to assess and improve an organization's third-party risk posture. The key enabler of accurate and actionable Cyber Risk Intelligence is the standardization of the data collected. Without standardization, it's impossible to utilize machine learning to perform analyses of the data.

CyberGRX is the Cyber Risk Intelligence industry leader. Within the CyberGRX Exchange, we have an unparalleled depth and breadth of data with more than 150,000 companies and 10,000 completed self-attested assessments. Eighty percent of the top 500 companies requested by customers are already on our Exchange. The use of standardized data to power our Exchange allows us to apply advanced machine learning to our data set, something that data sets derived from customized questionnaires cannot do. Because of these capabilities, we are able to produce unique insights across an entire portfolio of third parties. From inherent and residual risk views, to mapping against common and customized frameworks, to providing control gap analysis using threat profiles and attack analytics against real-life cyberattacks, we provide the most comprehensive and actionable risk profiles available.

The CyberGRX Predictive Risk Profile

CyberGRX harnesses the power of machine learning to produce Predictive Risk Profiles, unique insights across an entire portfolio of third parties using instant, predictive risk assessment results. Predictive Risk Profiles predict how a given vendor will answer each question in our standardized assessment based on firmographics, both outside-in data and inside-out data, and similar completed assessments on our Exchange with an accuracy rate of up to 85%. Each one of the 150,000 companies on the CyberGRX Exchange has a Predictive Risk Profile to view and share with those who request it, enabling transparency and collaboration to address control gaps and risk remediation strategies across an entire third-party portfolio.



Our sophisticated Predictive Risk Profiles allow companies to monitor and assess their third-party cyber risk through the lens that matters most to them. While the insights within these profiles can be used to assess and monitor a number of things within risk management and security programs, three distinct use cases can be applied to the Predictive Risk Profile in order to maximize the use of the data available and assist in decision-making.

How to use the Predictive Risk Profiles

Third-party risk management programs can be complicated, mainly due to the volume of information that needs to be processed as well as the complexities of having multiple stakeholders involved. Risk Management professionals need to be aware of which third parties are critical to business success and which ones threaten strategic objectives. Procurement professionals need a repeatable process to distinguish vendors requiring security due diligence from those that have no cyber relevance. Security personnel, on the other hand, need a single platform that consolidates threat intelligence, vendor identification, and risk scoring in order to meet business demands.

CyberGRX supports all teams involved in vetting third parties and managing their changing security postures through our Predictive Risk Profiles. These profiles provide valuable risk insights based on immediate, predicted assessment results for a third party as well as the full breadth of data within our Exchange. Your portfolio will benefit from the breadth of the CyberGRX Exchange immediately as third-party data will be available upon ingestion. CyberGRX can be jointly used with stakeholders both inside and outside the security team, which helps teams build an effective, streamlined third-party cyber risk management (TPCRM) program to aid in decision making for security, risk management, and procurement needs.

Predictive Risk Profile Use Case #1:
Existing Program Efficiency and Management

CyberGRX can help to improve efficiency and add real-time information into any third-party risk management program, enabling users to quickly understand how existing and proposed interactions with third parties can impact their business. Users can spend valuable time analyzing data and remediating risks discovered rather than chasing assessments.

The first step to managing third parties within the CyberGRX platform is to establish visibility of the third parties that are cyber relevant to the business. Using the Auto Inherent Risk feature and known firmographics, users automatically have crowd sourced inherent risk ranking for their third paties. They also can, and should, calculate the likelihood and impact of a cyber event by adjusting pre-populated answers focused on business exposure. The answers to these eight questions, whether automated or adjusted by the user, allow CyberGRX to sort third parties by high, medium, and low risk. This is determined by accounting for the type of business relationship with the third party as well as the access level to critical assets such as confidential data, networks, and facilities. This categorization is the fundamental tiering mechanism that segments the third parties and presents the Inherent Risk level of each vendor within the business' portfolio.

Once Inherent Risk is determined, users can begin to analyze vulnerabilities immediately and make informed decisions about where to prioritize risk management time and resources. Using both self-attested assessments on the CyberGRX Exchange and Predictive Risk Profiles, users can access the most comprehensive and actionable risk intelligence data available.

Beginning with those who pose the highest risk or most critical business exposure, a recommended approach is for a business to set a threshold for an acceptable level of residual risk. Risk thresholds can vary based on inherent risk scores, where more risk may be acceptable from low inherent risk vendors. Once the threshold is determined, the recommendation noted in the side bar could be employed to analyze which third parties (assuming high inherent risk for this example) need further exploration and validation and those that need no further exploration.

Setting thresholds to drive third-party cyber risk prioritization:

Begin by setting a threshold data point based on Predictive Risk Intelligence, such as 30*. Once all third parties are added to your portfolio in the CyberGRX platform, consider this approach:

- If attested results are significantly better than the threshold set in the Predictive Risk Profile values, request a follow up discussion and further validation.
- If attested results are the same as the threshold set in the Predictive Risk Profile values, no further validation is needed.
- If attested results are worse than the threshold set in the Predictive Risk Profile values, apply applicable frameworks and threat profiles from the Framework Mapper tool to gain a better view of specific control gaps.

* On a scale of 0-100 where 0 represents the lowest level of risk and 100 represents the highest level of risk, a typical risk threshold for a global enterprise using Predictive Risk Profiles might be 30.

Predictive Risk Profile Use Case #1 (Continued)

Beginning with those who pose the highest risk or most critical business exposure, a recommended approach is for a business to set a threshold for an acceptable level of residual risk. Risk thresholds can vary based on inherent risk scores, where more risk may be acceptable from low inherent risk vendors. On a scale of 0-100 where 0 represents the lowest level of risk and 100 represents the highest level of risk, a typical risk threshold for a global enterprise using Predictive Risk Profiles might be 30. Once the threshold is determined, the following recommendation could be employed to analyze which third parties (assuming high inherent risk for this example) need further exploration and validation and those that need no further exploration:

Predictive Risk or Residual Risk Score is above 30 out of possible 100:

Attested results available:

- Set up time to review assessments results with the third party to gain a better understanding of their security posture
- Request additional validation of assessment results
- Apply applicable frameworks and threat profiles from the Framework Mapper tool to gain a better view of specific control gaps to provide to internal SecOps teams

Attested results not available:

- Request validated assessment from the third party

Predictive Risk or Residual Risk Score is below 30 out of possible 100:

- Apply applicable frameworks and threat profiles from the Framework Mapper tool to gain a better view of specific control gaps to provide to internal SecOps teams

By defining an acceptable risk threshold, a company can reduce the overall necessity for validation and additional assessments, focusing resources on analyzing control gaps and threat profiles for these third parties to develop a more proactive threat response. Customizing the output using the Framework mapper tool provides the ability to adjust the lens through which a company can view third-party risk so that it best matches the risk they are most concerned with.

Predictive Risk Profile Use Case #2:

Building a third-party cyber risk management program

Building a third-party cyber risk management program can seem like a daunting task. Many organizations use consulting firms to get these programs off the ground, which is a viable option. However, those services can consume large amounts of time and money.

For those looking to build a third-party cyber risk program from scratch, the outdated approach is to create a customized assessment and send it to every third party within their ecosystem. But there are some problems associated with this approach. First, not all third parties are created equal and therefore assessing vendors with a "one size fits all" mentality can do more harm than good. Secondly, a process needs to be in place for collecting and, more importantly, analyzing the data received. This should be determined before assessments are sent to ensure that the volumne of data is able to be ingested in a way that is easy to use and provides insights. Third, an effective program should be focused on not only identifying areas of risk and control gaps but also providing a way to mitigate risk.

Taking these steps into consideration, Predictive Risk Profiles can be applied to a new TPCRM program to help build maturity and support long-term program effectiveness.

Establish vendor classification methodology

CyberGRX uses an Auto Inherent Risk feature to calculate the likelihood and impact of a cyber event through the answers to eight business exposure questions combined with known firmographics. Users can use the pre-populated answers or adjust as necessary to classify third parties by high, medium, and low risk based on the specific business relationship as well as the access level to critical assets, such as confidential data, networks, and facilities. This classification methodology is fundamental to tiering third parties and beginning the prioritization process.

View risk data through customized risk lenses

CyberGRX allows for immediate analysis of every third party in an organization's portfolio. Between our collection of more than ten thousand attested assessments and Predictive Risk Profiles for every third party on our Exchange, users can view control gaps immediately in order to make informed decisions about where to prioritize risk management time and resources. Once Inherent Risk has been determined, the next step is for an organization to identify those third parties which pose the highest risk and analyze their risk score. A similar approach to that described in Use Case 1 can be applied, starting with setting a threshold for an acceptable level of residual risk. Risk thresholds can vary based on inherent risk scores, where more risk may be acceptable from low inherent risk vendors. Once the threshold is determined, the following recommendation could be employed to analyze which third parties (assuming high inherent risk for this example) need further exploration and validation and those that need no further exploration:

Auto Inherent Risk score is less than or equal to 25:

- Do nothing except monitor over time

Auto Inherent Risk Score is between 26 - 75 and the residual risk is equal to or greater than 50:

- Review the attested assessment if available and address specific concerns with the vendor
- If there is no attested assessment, request one

Auto Inherent Risk Score is between 26 - 75 and the residual risk is less than 50:

- Review the attested assessment if available and request validation if needed
- If there is no attested assessment evaluate predictive data available, focusing on key predicted gaps that are of high concern
- Address specific concerns with the vendor regarding predicted gaps, and if necessary, order an assessment

Auto Inherent Risk Score is greater than 75 and the residual risk is greater than 25:

- Review the attested assessment if available and address specific concerns with the vendor
- If there is no attested assessment, request one

Auto Inherent Risk Score is greater than 75 and the residual risk is less than 25:

- Review the attested assessment if available and request validation if needed
- If there is no attested assessment evaluate predictive data available, focusing on key predicted gaps that are of high concern
- Address specific concerns with the vendor regarding predicted gaps, and if necessary, order an assessment

Predictive Risk Profile Use Case #2 (Continued)

View risk data through customized risk lenses

The final step in setting up the TPCRM program is to understand the most critical gaps based on your own risk tolerance and begin identifying opportunities to prioritize risk, working in collaboration with the third parties. Using the CyberGRX platform, you can:

- Identify the set of highest inherent risk third parties using the analysis tab.
- Identify the controls that are most important to your organization based on critical controls, threat profiles, etc. and overlay those controls against your third party set.
- Look for trends in identified risks within that third party/control set. For example, if all of these third parties are risky in a particular area such as password policies, the most efficient remediation may be to create controls or change processes within your own organization rather than trying to convince all third parties to take action.
- Collaborate with third parties regarding control gaps associated with the furthest "left" techniques in cyber kill chains using the Attack Scenario Analytics built on MITRE ATT&CK® Framework. Those controls will help stop attacks soonest.

The difference between an ad-hoc approach and a more mature, managed approach:

Ad-Hoc	VS	Managed
Vendor classification methodology not established		Vendor classification is automated & repeatable
Assessments are mostly data collection with little analysis of responses		Responses are streamlined in collection and are analyzed to provide actionable insights
Identified gaps are not prioritized		Gaps are identified and prioritized to better support remediation efforts

Predictive Risk Profile Use Case #3:
Third-Party Selection and Contract Negotiation

CyberGRX supports all teams involved in third-party selection and contract negotiation through Predictive Risk Profiles which provide immediate, predicted assessments results for a third party. By being able to review security and risk posture data, including control gaps and compliance posture, teams gain valuable insights that aid in contract negotiations by requiring third parties to remediate risks prior to contract acceptance and onboarding.

Procurement, Risk Management, and Security teams can vet new third parties prior to onboarding by reviewing Predictive Risk Profiles. These profiles provide valuable risk insights based on immediate, predicted assessments results for a third party. To use this feature as part of the vetting or onboarding process, a company can take these steps:

- Add the third party or parties to their company portfolio in the Portfolio Management tab
- Review key findings and immediate outside-in scanning intelligence on the Summary tab
- Review each third party's Predictive Risk Profile available under the Assessment tab focusing on the Predicted Coverage rating.
  - A best practice is to look for a high confidence combined with low coverage in order to have a better understanding of where the potential risk may be.
  - An example could be a new benefits vendor being requested by HR. This vendor would have access to employee Personally Identifiable Information (PII) which means focusing on the coverage of privacy and data protection controls is most critical. If the vendor has high confidence of low coverage, then the evaluating team may consider deeper inspection of their privacy policy and website certifications which could lead to a denial of the purchase or a need to request more information. If there is high confidence with high coverage, potential risk most likely will be lower, and the team may feel more confident moving forward.

CyberGRX can be jointly managed with stakeholders both inside and outside the security team, which helps teams build an effective, streamlined third-party cyber risk management program to aid in decision making for procurement, risk management, and due diligence use cases.

Third Parties are a top attack vector

The use of third parties continues to be necessary for organizations in the growing digital economy, with the average enterprise organization using close to 5,800 vendors. With this reliance comes an increased vulnerability to cyber threats, specifically ransomware and supply-chain focused attacks. Recent attacks on software providers, managed security providers, and credit agencies are perfect examples of the dangers these third-party attacks pose. Rapid decision making is critical to both an organization's success as well as their threat posture. By providing immediate access to third-party intelligence and Predictive Risk Scores, Procurement, Risk Management, and Security teams using CyberGRX can better support the needs and security of their organization.

Conclusion

Frustration around third-party cyber risk management stems from a broken process. Through the application of Cyber Risk Intelligence, CyberGRX is revolutionizing this process. The self assessment, while a piece of the puzzle, no longer has to be the first step to determining the risk posture of your third parties. Through the use of standardized data that makes up the world's first and largest third-party cyber risk Exchange, organizations can finally begin to view their third-party risk through the lens that matters most to them, better decisions faster, and implement a TPCRM program that delivers ROI immediately upon launch, not once assessments are collected.