Cyber GRX

VOLUME ONE

CyberGRX Exchange Insights

From the CyberGRX Data
& Analytics Team

A Data Visualization of the CyberGRX Exchange

Each dot represents a company or third-party assessment.

Introduction

Participants on the CyberGRX Exchange work together in a one-to-many fashion to crowdsource data, insights, and remediation strategies. With over 80,000 third parties ingested and nearly 4,000 third parties assessed, we're using this important data to inform the industry and organizations around the world of third-party risk insights and trends.

About the Authors

Adam Gray is a Data Scientist at CyberGRX and earned a Ph.D in Mathematics from the University of Mississippi in 2010. His research interests include combinatorics, graph theory, matroid theory, machine learning, algorithms, and data science.

Joe Marques is a data miner, software architect, and high-performance computing expert with a background in cybersecurity, biometrics, and identity management systems. He earned a BS in Computer Science from the University of Delaware and currently holds two patents.

Dan Tobin is the Analytics Director at CyberGRX and earned a Master's in Mathematics from the University of North Carolina at Wilmington in 2003. His interests include big data engineering, data science, operations research, and natural language processing.

Aser Garcia is a Data Science intern currently enrolled in CU Boulder's Statistics and Data Science Master's program.

Atreyee Sen is a Data Science intern currently pursuing her Master's in Information Technology and Management at The University of Texas at Dallas specializing in Data Science and Analytics.

Insight 1

Twenty Percent of an Organization's Third Parties are High Risk.

Based on the third-party population ingested by enterprise customers, on average, **20% of an enterprises' third-party portfolio pose high inherent risk**. This means that if these third parties become compromised or unavailable, the fallout of that event will have a high impact on the enterprise. Unlike Residual Risk, Inherent Risk is the risk absent any security controls, but it is critical in helping organizations identify who to focus their due diligence efforts.

METHODOLOGY

Impact and likelihood are determined in two ways: We build profiles on third party types using a combination of responses to eight business impact questions the enterprise completes and our automated inherent risk tool, then applies machine learning across that data with CyberGRX AIR Insights™. AIR Insights compiles a business exposure score based on how similar third parties have been rated before and their Thomson Reuters business classification.

Why this Matters

According to a **2020 Ponemon** survey, the typical enterprise has an average of 5,800 third parties, and because of that significant level of risk, there should be some level of due diligence. Furthermore, the number of third parties that organizations use is expected to grow by 15 percent in the next year. The study found that the biggest impact on cyber risk was the increased reliance on third parties, like cloud providers, IoT and Shadow IT. So, the challenge of keeping your organization safe will only continue to grow.

Cyber GRX

Ponemon Institute

Digital Transformation & Cyber Risk: What You Need to Know to Stay Safe

Sponsored by CyberGRX

Independently conducted by Ponemon Institute LLC

PUBLICATION DATE - JUNE 2020

In addition, **another Ponemon study** found that over 50 percent of organizations believe they are ineffective at conducting the due diligence on their current third parties. If your third-party security isn't on your radar or it isn't a top priority, we are giving you a few reasons why it should be—sooner rather than later. Our collective reliance on third parties isn't going away, and the first step to a mature third-party program is simply identifying who your third parties are and understanding their inherent risk. Once you know which ones pose you the most inherent risk, you can move forward with due diligence and assessing to determine if they have the proper security controls in place to mitigate that risk. But you have to start somewhere, and we believe that is inherent risk.

Insight 2

Third Parties in Certain Industries are More Likely to Have Mature Cyber Security Programs, But Still Have Significant Gaps.

Organizations in the Financial, Technology, Telecom, and Healthcare industries are oftentimes third parties themselves. **Our data shows that these third parties tend to have strong controls in place to mitigate risks** associated with incident containment, threat removal, and identity authorization and authentication.

METHODOLOGY

Third-party cyber risk management affects all companies, yet according to our data, companies in the Financial, Healthcare, and Telecom sectors tend to have more mature security programs.

Financial, Healthcare, and Telecom companies tend to also be strong in network security protection, while Financial and Telecom companies tend to be strong in network content protection. Conversely, Energy, Consumer Cyclicals and Consumer NonCyclicals have the least mature programs. At the same time, organizations in all these industries are typically weak in controls around desktop and laptop protection, server protection, and virtualization protection.

We evaluate an organizations' vulnerability and risk by assessing both their overall security control coverage (e.g. do they have controls in place to mitigate common risks and attack paths) as well as the maturity and sophistication of their program (e.g. company's ability to sustain positive cyber practices and improve them over time). We determine security maturity by asking seven questions about the people, processes and technology in place for each of the 5 control groups: Strategic, Operational, Core, Management and Privacy.

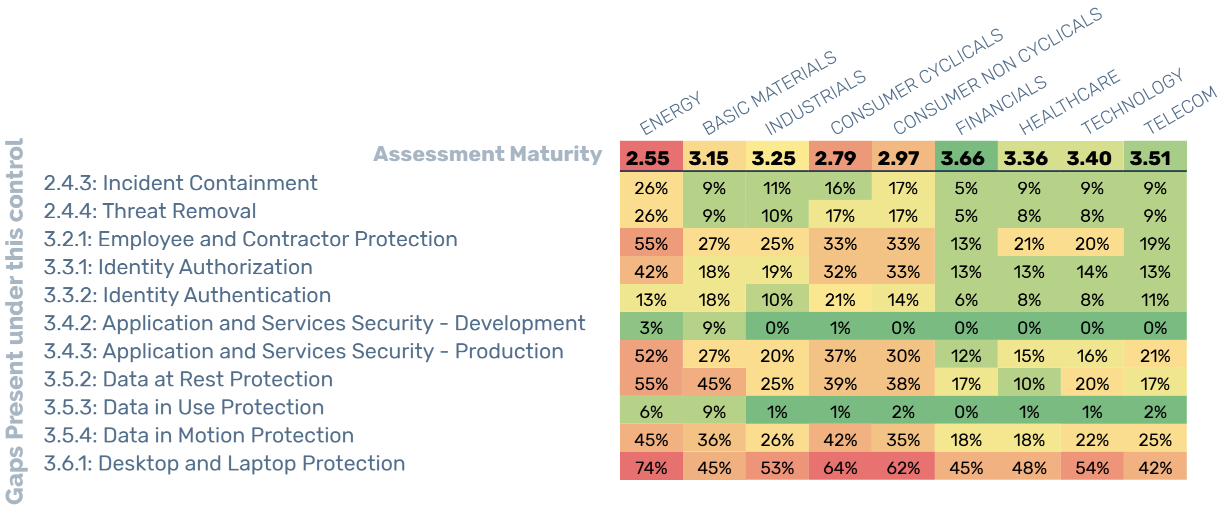
For Example:

People – The level of maturity in staff roles, experience, education, and training

Process – The level of policy and procedural maturity

Technology – The level of maturity related to the use of technology tools and related data

We then rate maturity on a scale of 0-5 with 5 being the most mature, or having programs that are efficient, scalable, and adaptable. Higher maturities often indicate that a company can better maintain a robust cybersecurity posture in the context of changing business conditions, employee turnover, and financial challenges. Low maturities make it more difficult to adapt to changing conditions and call into question the sustainability of good security controls when they do exist.



Gaps Present under this control

	ENERGY	BASIC MATERIALS	INDUSTRIALS	CONSUMER CYCLICALS	CONSUMER NON CYCLICALS	FINANCIALS	HEALTHCARE	TECHNOLOGY	TELECOM
Assessment Maturity	2.55	3.15	3.25	2.79	2.97	3.66	3.36	3.40	3.51
2.4.3: Incident Containment	26%	9%	11%	16%	17%	5%	9%	9%	9%
2.4.4: Threat Removal	26%	9%	10%	17%	17%	5%	8%	8%	9%
3.2.1: Employee and Contractor Protection	55%	27%	25%	33%	33%	13%	21%	20%	19%
3.3.1: Identity Authorization	42%	18%	19%	32%	33%	13%	13%	14%	13%
3.3.2: Identity Authentication	13%	18%	10%	21%	14%	6%	8%	8%	11%
3.4.2: Application and Services Security - Development	3%	9%	0%	1%	0%	0%	0%	0%	0%
3.4.3: Application and Services Security - Production	52%	27%	20%	37%	30%	12%	15%	16%	21%
3.5.2: Data at Rest Protection	55%	45%	25%	39%	38%	17%	10%	20%	17%
3.5.3: Data in Use Protection	6%	9%	1%	1%	2%	0%	1%	1%	2%
3.5.4: Data in Motion Protection	45%	36%	26%	42%	35%	18%	18%	22%	25%
3.6.1: Desktop and Laptop Protection	74%	45%	53%	64%	62%	45%	48%	54%	42%

INSIGHT 2: CONTROL DATA

Examples of control data presented as gaps present under the control and averages for various industries in relation to those gaps.

Why this Matters

The data is showing that companies in certain industries are more likely to have significant gaps in their cyber security programs and it's important that organizations do their due diligence. Understanding the different risk can be helpful in identifying, prioritizing, and reducing cyber risk.

Insight 3

Company Size Correlates With Security Maturity and Coverage.

Our evaluation of third parties measures the existence and effectiveness of security controls to mitigate risk as well as the overall maturity of the third party's security program. **As companies get smaller, they have fewer controls in place and less mature programs.**

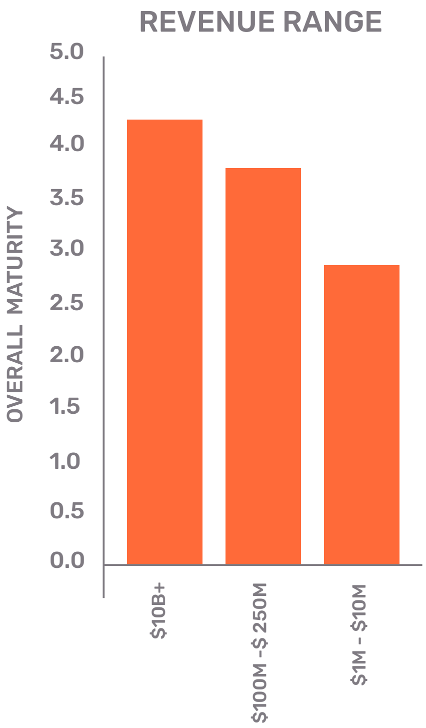
METHODOLOGY

Control coverage is an indication of which Strategic, Operational, Core, and Management controls a third party has in place. Strategic controls address cybersecurity and privacy policies, planning, and governance. Operational controls cover everyday security activities such as threat analysis, incident response, and vulnerability management. Core controls are made up of technical safeguards like data encryption, key management, and endpoint protection. And finally, Management controls focus on security-related processes or functions such as configuration and change management or third-party risk management.

When we break down each of these control groups, we find the greatest disparity in coverage by company size in the Management and Core control groups. Overall, companies with $100M to $10B in revenue have similar coverage levels in terms of Strategic and Operational controls (approaching 100% coverage). However, companies with $1B revenue and above had greater coverage of Core (95%) and Management controls (100%) versus their counterparts in the $100M-$250M range who have 90% coverage of Core controls and close to 95% coverage of Management controls.

The real difference comes when we look at smaller companies. For instance, companies with revenues of $1M-$10M had lower coverage across all control groups, particularly in Core controls (82%) and Management controls (78%).

Overall maturity levels also decline as company revenue decreases. We determine maturity level by asking seven questions that evaluate the people, processes, and technologies that impact the efficacy of each security control group. We then rate maturity on a scale of 0-5 with 5 being the most mature, having programs that are efficient, scalable, and adaptable. The overall maturity for companies with $10B or more in revenue is 4.4 out of 5. As you move down in revenue to the $250M range, maturity drops to 3.8 and if you continue down to the $10M revenue range, maturity drops to 2.9. Across the CyberGRX Exchange of assessed third-party companies, the average maturity level is 3.5.

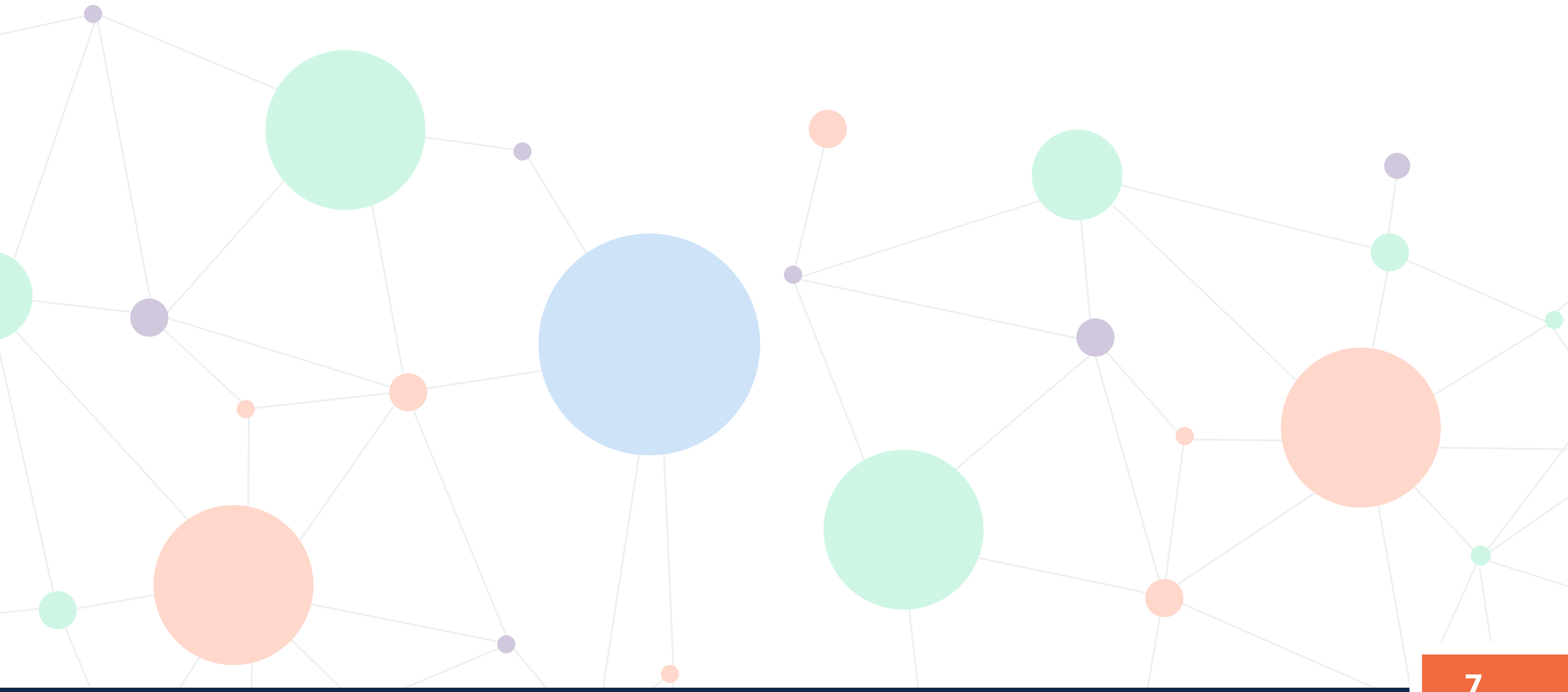


INSIGHT 3: REVENUE RANGE

Showing the overall maturity of assessment data vs. company revenue

Why this Matters

This is interesting because many organizations tend to focus their security due diligence efforts on larger third parties. But larger organizations do not necessarily equate to greater risk. While all third parties require some level of due diligence, it is important to engage with the small and mid-sized third parties that you may have assumed pose less risk. These third parties can have significant access to sensitive data and systems, and as our data shows, they often are less mature and have lower levels of security control coverage.



Insight 4

The Most Common Third-Party Security Gaps are Desktop and Laptop Protection, Server Protection and Virtualization Protection.

We assess a third party's strength and weaknesses across five control groups: Strategic, Operational, Core, Management, and Privacy. The questions we ask around Operational and Core controls are directly related to threat use cases and kill chain analysis, and those results provide tangible gaps and risks that should be remediated to reduce risk exposure.

Based on an aggregated view of all completed assessments in our exchange, the top five weakest control areas across all industries are listed below from high to low:

Desktop and Laptop protection

The lack of desktop and laptop security controls means that third parties are vulnerable to attack at their most distant user endpoints. For example, attacks that target unencrypted hard drives, session hijacking, and opportunities for the installation of malware are all risks that these third parties face. This is particularly troubling given the rapid adoption of remote working that has resulted in a situation where these endpoints are less likely to be protected by an organization's traditional network security safeguards.

Server protection

These controls deal specifically with physical server assets. Servers are often the backbone of an organization's computing environment and provide several functions including hosting web sites, serving applications, and storing databases. There are myriad threats and risks that could result from server-related vulnerabilities including the possibility of successful ransomware attacks, unauthorized data exfiltration, and website defacement.

Virtualization protection

The past decade or two have seen an incredible increase in the utilization of virtualization as the standard computing and data storage solution for organizations of all types, due to the adoption of cloud services provided by solutions like AWS, GCP, and Azure. Almost every IT asset can be virtualized which means that a lack of security protections in this area can have an enormous impact. Everything from unauthorized access to widespread malware attacks are real possibilities when virtual assets are not properly protected.

Data at rest protection

The protection of data is a primary objective of security. Organizations' responsibility to ensure the security of their data does not end when they share that data with a third party. The fact that third parties struggle with basic data protections such as encrypting data at rest should be alarming for all parties. Encryption is a fundamental security control that can be the key safeguard preventing the exfiltration and malicious use of sensitive data such as personally identifiable information (PII).

Data in motion protection

When we share data externally, we are generally connecting to third parties over the internet. If the transmission of information is not encrypted it opens the door for anyone "listening" to freely access, store, and use our sensitive data as they wish. In addition, a malicious actor may also modify the data en-route to achieve their objectives. Much like the encryption of data at rest, this is a basic security control that should be considered mandatory.

Insight 5

Organizations Tend to Focus on the Same Set of Vendors, But it is Often the Vendors They Aren't Looking at That Pose the Greatest Risk.

Since 2015, CyberGRX has been collecting data on the cyber security practices of organizations and third parties around the world. Over the years, as the CyberGRX exchange has grown in diversity, size, and scope as customers have reached deeper into their third-party ecosystems and requested assessments on a broader set of companies. Furthermore, **companies with a history of assessments have been incentivized to improve.** Using feedback from the platform, they have addressed key control gaps and mitigated them in later assessments.

METHODOLOGY

Modern and scalable approaches are allowing companies to look deeper into their portfolio of third parties, and if you have built a program that only reviews the larger, top companies, you are likely missing a higher concentration of risk from weaker controls from the next layer of companies - companies that may have similar data access and thus pose a higher risk.

This is one of the main reasons why it's important that enterprises are able to dig deeper than the first level of their vendor ecosystem to start addressing this exposure and ultimately build more mature and comprehensive TPCRM programs. By using an assessment Exchange, companies can move on to deeper layers of their vendor ecosystem that they did not typically assess or evaluate. The result is a lot of risk and exposure that otherwise wouldn't have been uncovered had the organization not been able to quickly assess their first level vendors.

Why this Matters

Don't always assume the first layer of third parties have the most risk. These companies tend to be larger and have a more mature TPCRM program in place. It's the companies that are two and three layers down that pose significant—and oftentimes unseen—risk. With the right scalable and repeatable approach that allows you to quickly and efficiently move past the top-level third parties, you can identify and mitigate potential risk before it becomes a problem.

How Does CyberGRX Get its Data?

CyberGRX collected this data by examining the most recent assessments for companies in the exchange and aggregating results into the industry sector that each company primarily services. The risk analysis used to measure inherent risk and identify control gaps relies on a custom database of threat use cases derived from a broad set of government, academic, and industry sources. These tie together threat actors, their intended outcomes, and a series of kill-chain stages employed during the attack. The kill-chains are based on the MITRE ATT&CK framework with its related taxonomy and are linked back to the controls in the CyberGRX assessment that could mitigate them. CyberGRX performs a graph-based analysis of the applicable use cases for a company's industry, their assessment answers, and a series of scoping responses to determine how customers engage with their third parties across eight asset types (see AIR Insights™). These algorithms surface the control gaps and other risk metrics that are most relevant to each third party.