USTELECOM
THE BROADBAND ASSOCIATION

Improving the Quantitative Cybersecurity Ratings Assigned to Telecommunications Firms by Commercial Vendors

JANUARY 2024

PREPARED BY

Mr. Robert Mayer
Senior Vice President,
Cybersecurity & Innovation
USTelecom

Dr. Edward Amoroso
Chief Executive Officer,
TAG Infosphere
Research Professor NYU Center
for Cybersecurity

Executive Summary

Over the past many years, a group of cybersecurity rating firms have developed proprietary methodologies that produce rankings for individual enterprises relying largely on publicly available scans of their internet- facing assets. While these scores can provide important insight on a company's risk posture, the methodologies employed to achieve these outputs have raised significant concerns when the assets evaluated are not controlled by the surveyed entity. These methodological flaws are particularly problematic for telecommunications firms and Internet Service Providers (ISPs) that provide their customers with blocks of IP addresses for use in their own organizations or for the customers. This problem has been known for many years and as the use of cybersecurity scoring services continues to grow, so have the harms associated with their often-misleading conclusions.

Since at least 2018, the rating firms have been aware of these concerns and at least one major scoring company made a substantial concession when the U.S. Chamber of Commerce and FICO Cyber Score (since acquired by ISS) revised their industry benchmarking initiative, (the Assessment of Business Cybersecurity (ABC). In a subsequent report, they acknowledged that ISPs, Infrastructure as a Service (IaaS), telecom, and cloud service providers "...with large IP address footprints controlled by IT and security teams outside their direct control could increase the likelihood of double-counting assets when such assets would be more appropriately attributed to the subscribing organizations." They explained that "[F]or these reasons, we have elected to exclude companies in this class and have adjusted the ABC and its various sub-indices."

This report is intended to provide an update on progress in this area and focuses on issues that continue to plague telecommunications firms and ISPs that must make substantial and ongoing investments to segment massive sets of IP addresses. The report describes the quantitative mechanisms that are used and why they continue to be a source of disagreement between telecommunications firms and security rating vendors. The rating company business model is also critiqued and while it acknowledges the value that fair and methodologically supported mechanisms can offer a variety of stakeholders from Boards to procurement specialists evaluating third-party risk, it offers three constructive recommendations to advance the interest of all parties.

First, the report notes that its purpose is not to make algorithmic design decisions for the security rating companies. Instead, it urges these companies to consider alternatives for "asset discovery" in ways that improve the validity and accuracy, and thus the utility of their products. Second, the authors explain why the rating firms should provide an option for customized risk models based on the unique characteristics of telecommunications firm's' threat landscape and business use cases. And third, the rating firms are encouraged to engage proactively and collaboratively with customers to improve rating accuracy. It notes that by working in such ways with the telecommunications providers, the rating firm would benefit from continuous improvement in a very dynamic cyber ecosystem.

Finally, the report notes that initial communications with leading ratings providers have already produced positive results. As evidence of such progress, both BitSight and Security Scorecard removed their industry scores from their public-facing websites industry scores for telecommunications firms.

The objective of this report and the research that supported its development is to help coordinate enhancements to these security ratings and the associated ecosystem, as well as to help to stimulate additional and on-going cooperative partnership between telecommunications firms, ISPs, and the commercial vendors working in this area of cybersecurity posture quantification.

Background

Since 2018, several groups including the U.S. Chamber of Commerce, FICO, ETNO,[1] and USTelecom[2] have reviewed the growing industry of cybersecurity risk ratings. Each of these studies has concluded that while security ratings are important and provide value for boards, investors, underwriters, and third-party risk management (TPRM), the accuracy and correctness of ratings algorithms can and should be improved to avoid unintended reputational issues for telecommunications firms and Internet Service Providers (ISPs).

To illustrate the problem, consider that proxy advisory services companies who score Environmental, Social, and Corporate Governance (ESG) for publicly traded companies have begun to use security ratings to grade a company's cybersecurity program and to determine corporate ESG scores.[3] The financial community is thus now using these scores for market investment decisions, and recent SEC rulings have removed the obligation for proxy advisory companies to notify the target company before publishing their findings and recommendations.

The result of this and other usage of security ratings creates considerable friction for telecommunications companies and ISPs with various stakeholders, including their customers. Experience shows that telecommunications firms and ISPs must spend considerable time and effort answering questions from enterprise and government customers to explain why their published scores might be inexplicably low—generally as a result of algorithmic deficiencies in the ratings calculations (explained below). While such customers might understand the rationale, such interactions introduce business risk, including the potential for revenue loss.

The primary goal of the work described in this report[4] is to provide a comprehensive and updated summary of the remaining issues associated with commercial ratings for telecommunications firms and ISPs, and to recommend several practical near-term approaches to help address the challenge of solving this problem. The report is based on a detailed review of previous analyses, one-on-one discussions with many different domestic telecommunications firms and ISPs, and recent reviews held with several of the major commercial cybersecurity ratings vendors.[5]

Basis for Cybersecurity Ratings

It is well-established that quantitative cybersecurity ratings from commercial vendors are intended to offer a common and objective means to assess and compare the cybersecurity posture of different organizations. Such ratings are designed to address the growing need for businesses and other stakeholders to have a better understanding of the cybersecurity risks associated with their own operations, as well as those of their partners, vendors, and other third parties.

Establishing such understanding is obviously a multidimensional activity and cybersecurity ratings do not remove the need for any team to review aspects of their own cyber protection ecosystem, or the ecosystem

of suppliers, partners, or other entities, based on local specifics or conditions. Ratings are intended instead to complement, augment, and contextualize such work with emphasis on the externally observable aspects of a target environment.

Quantitative ratings are created using proprietary algorithms that utilize a wide range of cybersecurity-related data gathered and derived from various sources, including public information, Internet scanning, network behavior analysis, review of visible settings such as Domain-based Message Authentication, Reporting, and Conformance (DMARC),[6] and more. Such telemetry and data are then analyzed and processed to generate a more comprehensive view of an organization's cybersecurity posture.

A major aspect of commercial cybersecurity risk rating algorithms includes identification of a range of Internet protocol (IP) addresses and domain names for a given company. This prompts a network scan of the public infrastructure in the target company's range for known security vulnerabilities. Proprietary quantification algorithms are then used to determine the target company's final cybersecurity score. We mention this address scanning component because it represents a major point of disagreement between telecommunications firms and security ratings vendors (see below).

As suggested above, security ratings are useful in many different contexts. For example, every organization, including telecommunications firms and ISPs, relies on external vendors and third parties to support day-to-day operations. Gaining insight into the cybersecurity posture of these entities through ratings can help prevent security breaches. Similarly, for mergers and acquisitions (M&A), businesses must evaluate the cybersecurity readiness of the companies they plan to acquire. Ratings offer a layer of added due diligence for M&A teams.

It is worth mentioning that cybersecurity has also become a critical concern for executives and board members, including ones without technical backgrounds. Ratings, if done properly, can provide an easily ingested number that can be used to communicate security status and improvements. Ratings might also be useful to include in cyber reporting obligations such as with recent requirements levied by the Securities and Exchange Commission (SEC),[7] but this remains to be confirmed in practice.

Other areas where security ratings are helpful include support for the cyber insurance industry, where providers can use quantifications to assess risk and set premiums. Ratings also allow organizations to benchmark their externally visible security performance against industry standards and competitors, which can help to identify areas for improvement and measure the effectiveness of on-going cybersecurity initiatives.

Transparency and accountability are among the most important aspects of security ratings that most business and government stakeholders value. This includes the customers, investors, and partners of a rated organization since all are increasingly concerned about cybersecurity. Publicly available ratings do much to enhance the transparency of security posture and help to demonstrate an organization's commitment to cybersecurity.

Readers should note that we go to great lengths above to identify and reinforce that our position is not to remove or discontinue the general use of cybersecurity ratings from commercial vendors. Rather, we intend to point out the algorithmic inconsistencies that emerge when trying to assign a single numeric value on

an ordinal scale to massively complex telecommunications firms and ISPs, especially when their business includes providing IP infrastructure for hundreds of thousands of other businesses being rated by these same cybersecurity firms.

Summary of Issues Raised by Telecommunications Firms and ISPs

As suggested above, telecommunications firms and ISPs have raised several issues to date with respect to security ratings and the degree to which these quantifications accurately reflect their business.[8] As any participant or observer of cybersecurity knows, telecommunications firms and ISPs provide the underlying network foundation on which all businesses, government agencies, consumers, families, and any other group or organization establishes its digital ecosystem, and this includes cloud services and software-as-a-service (SaaS) applications.

Telecommunications firms and ISPs are different from normal enterprise companies in many ways relevant to the manner in which cybersecurity ratings are developed. First, the business of such firms is to support the external networking and infrastructure posture of their customers through the provision and support of network services. The result is that external views of telecommunications firms and ISPs are often intertwined with the external views offered by their customers. This creates inaccurate views of the provider's security posture—somewhat akin (using a non-technical analogy) to holding a landlord responsible for how their tenants might be arranging their furniture.

Second, telecommunications firms and ISPs are incredibly complex entities from a network perspective since networks *are* their products. As such, the challenge to represent the security posture for such massively complicated organizations into a single, numeric figure of merit is considered by many in the industry, including these authors, to be highly misaligned. As suggested above, this is not to say that ratings cannot be used for large companies, but the business of a telecommunications firm and ISP is so complex from an external network perspective, that it calls into question the feasibility of generating a single accurate rating.

Below, we outline the three major issues we've collected through direct discussions with telecommunications firms and ISPs during 3Q2023 regarding cybersecurity ratings in this industry. Our interactions were mostly with senior representatives from this industry including Chief Information Security Officers (CISOs) and senior executives with security policy and legal responsibility. Major domestic Tier 1 providers were interviewed, but the names of the principals are not listed here as per agreed-upon sharing protocol.[9]

Issue 1: Security Ratings and IP Address Management

Telecommunications firms and ISPs justify their significant concerns regarding security ratings and how they are influenced by externally visible attributes of their IP address management based on the following technical and operational considerations:

1. *Limited Control* - Providers have a large number of IP addresses under their management due to the vast number of customers they serve. Furthermore, managing these IP addresses involves dynamic assignment to users. Providers explain that they do not have direct control over the behavior of all devices connected to their network. This leads to misattributions of security issues in the commercial ratings algorithms.

2. *Customer Responsibility* - The majority of security incidents associated with a telecommunications firm or ISP will occur due to actions taken by their individual customers. This involves running vulnerable software on a connected device or having one of their employees fall victim to a phishing attack, thus leading to a break-in at some designated address or domain. As per contractual agreements, providers simply do not prevent such user-level behavior.
3. *Botnet Infections* - IP address-based security ratings might falsely label a provider as insecure due to the presence of devices infected by malware or participating in botnets. Providers cannot stop their customers from connecting compromised devices to their networks, and these devices could easily be generating malicious traffic without the provider's knowledge or involvement. Again, this is dictated by contract.
4. *Misleading Metrics* - Relying solely on IP address-based security ratings can create a misleading picture of a provider's cybersecurity posture. These ratings often focus on factors like open ports, vulnerabilities, or other observable metrics—again, associated with IP allocations to customers. Such metrics, it might be added, usually neglect more nuanced security practices and internal measures that an ISP might have in place.
5. *Lack of Context* - Security ratings algorithms lack context about the provider's internal security policies, practices, and the efforts they invest in maintaining a secure network. These algorithms do not consider the various layers of security, including firewalls, intrusion detection systems, and traffic monitoring, that telecommunications firms and ISPs employ to safeguard their infrastructure.
6. *Dynamic Nature of Networks* - Networks are dynamic environments where devices and configurations change frequently. An IP address that might be flagged as insecure at one moment could become secure after necessary mitigation measures are taken by the provider. Static snapshots provided by security ratings do not capture this dynamic aspect accurately.
7. *Unaccounted External Factors* - Security ratings algorithms often don't integrate external factors that can impact a provider's cybersecurity such as upstream attacks, sophisticated threats, or the evolving threat landscape. These factors can affect the security rating but might be beyond the telecommunications firm or ISP's immediate control.

Issue 2: Ratings Company Business Model

A second major issue that emerged during virtually all interviews with telecommunications firms and ISPs involved the business model for cybersecurity ratings companies.[10] In short, the concern was that while security ratings are increasingly being viewed as external and presumably unbiased quantifications of cybersecurity posture, the primary means by which improvements, adjustments, or even insights into the ratings assigned a provider can only be done under contract.[11]

The result might be a perception of a pay-to-play view of the ratings companies from a provider perspective. No telecommunications firm or ISP suggested that such vendors should not approach these providers for a potential commercial relationship, and every provider acknowledged the local usefulness of cybersecurity ratings for third party risk management (TPRM), M&A due diligence, and security support for external partner or other stakeholder ecosystems. This was universally agreed upon, which would seem to be good news for the security ratings companies.

The idea, however, that a rating assigned to a provider for its own infrastructure should receive a lower priority for attention was cited often as a major impediment. This is underscored, as suggested above, by the increasing use of ratings in various government filings and other contexts where such rating is assumed to have been done under standard and unbiased circumstances. The common view is that ratings companies should adjust their business model; perhaps offering concierge treatment for telecommunications firms and ISPs was a repeat theme during our research with these providers.

Issue 3: Improved Ratings Approach for ISPs

A third issue that emerged during virtually all discussions was the view that a single number, namely, a single, quantified figure-of-merit rating, offered an insufficient representation of the cybersecurity posture of an entity as complex as these types of providers. Every discussion included some anecdote about comparison of their telecommunications firm or ISP rating to some entirely different entity (e.g., a small business) using the common ratings scale.

The view was frequently shared that providers should be considered in their own special category for ratings agencies. Ideas shared ranged from extending the ratings to a series (*i.e.,* linear vector) of ratings in various categories to the development of ratings categories which might designate a telecommunications firm or ISP as being within some equivalence class (*e.g.,* world class, mature, moderate, etc.). This would remove providers, for instance, from the same ratings scale and range as smaller entities.

It was also discussed that coordination between ratings vendors and providers should be more consistent, on-going, and dynamic. The inevitable discussion about whether ratings agencies should be given data about internal operations was raised by this author, but usually not met with great enthusiasm. This is obviously an area in which the ratings companies would like to see progress, but some work will be required to convince telecommunications firms and ISPs of the benefits and usefulness.

One area of our research worth mentioning is that considerable work was done reviewing the pros and cons of security ratings versus maturity models such as from the National Institute of Standards and Technology (NIST) Cybersecurity Framework,[12] International Organization for Standardization (ISO) Standards, and the Center for Internet Security (CIS) Controls. While many details emerged of the relative advantages and disadvantages of each approach, we would not presume to suggest that the business models of the ratings companies should change.[13]

Strategic Advice for Ratings Vendors

Below we outline several ways in which cybersecurity risk rating providers might take steps to improve the trust among their customers across the telecommunications and ISP landscape. Specifically, we make recommendations below in the areas of Asset Discovery, Risk Model Customization, and Stakeholder Engagement.

Recommendation 1: Asset Discovery

Today, most commercial cybersecurity ratings vendors use the American Registry for Internet Numbers (ARIN) to collect information on a given company. As most industry experts will attest, IP registrations change quickly, and the result is that the accuracy of the ARIN database is often in question. In addition, ARIN is susceptible to fraud and illegal activity, which can lead to inaccurate data and improper attribution.[14]

As stated above, this presents particular problems for telecommunications firms and ISPs that are rated based on IP address information that is both not under their direct control but might also be potentially incorrect in the context of customer usage. Admittedly, this issue of ARIN accuracy applies much more generally than for just telecommunications firms and ISPs, but it is certainly worth mentioning as an area for improvement by ratings companies.

One potentially more accurate method for conducting IP-based asset discovery is to cross reference root domains and associated sub-domains and Fully Qualified Domain Names (FQDNs) against a company's domain name system (DNS) records, which are actively maintained, and then perform reverse IP lookup.[15] This approach could minimize misattribution or missed assets. This approach could also have the additional benefit of identifying stale or misconfigured DNS settings.

While we do not view our purpose here as making design decisions for the security ratings companies that have extensive experience and expertise designing algorithms, we do think reviewing alternatives for asset discovery to be a worthwhile activity. The approach suggested above, for example, has the advantage of mimicking how threat actors perform reconnaissance and, while it could require more effort than an ARIN search, it could also provide better results.

Some questions we recommend security ratings companies consider in the context of improving their process for IP-based asset discovery include the following:

1. Do you provide clarity and transparency regarding the algorithms that implement your asset discovery process?
2. Does your algorithm include provision to accurately differentiate between provider-owned vs. customer-owned IP addresses and assets?
3. Do you have a process for addressing potentially misattributed assets, either through a new calculation or a change to the processing model?

Recommendation 2: Customized Risk Model

In the course of our investigations and research with the telecommunications firms and ISPs, the idea emerged that a so-called *customized risk model* might be considered for use. The driver here is that cybersecurity risk rating models might not be well-suited to a single, common application across all providers. Such a "one-size-fits-all" approach would miss the complexities that differentiate different providers.

The way this might be done would involve allowing cybersecurity risk rating clients, including telecommunications firms and ISPs, to have the option to adjust their cybersecurity risk rating models based on the

uniqueness of their local threat landscape and use cases. This would ensure that the resultant rating is more pertinent to their mission, subsidiaries, acquisitions, divestitures, departments, and third parties.

Cybersecurity risk providers already tend to employ numerous factors in their calculations. This is evident in that vendors often determine factor weights and thresholds at their own discretion, thus leading to different cybersecurity risk rating providers providing different scores for the same company. This establishes precedent that adjustments to a rating could be locally determined based on expert insight into the specifics of a target environment.

Some questions we recommend security ratings companies consider in the context of improving their cybersecurity risk models include the following:

1. Would you consider options to customize a risk score? Could the factors used to create the score be adjusted in the weighting and thresholds?
2. Do you provide transparency into the specific factors that go into your individual rating and the relative weighting of the factors in the score?
3. Which of the following additional elements are embedded in your analysis to produce a comprehensive risk score: Internal vulnerabilities, internal risks, external vulnerabilities, external risks, cloud security risks, third-party vulnerabilities and risks, and human risk?

Recommendation 3: Stakeholder Engagement

Based on our analysis, we encourage the commercial rating providers to engage proactively and collaboratively with their telecommunications and ISP customers to improve rating accuracy. In our research, we found that some rating providers might be less inclined to proactively engage customers to enhance their rating accuracy. This is unfortunate, because by working with the provider segment, rating providers can use the collaboration to drive continuous improvement.

Key aspects of such stakeholder engagement would include on-going information sharing sessions between providers and ratings companies, collaboration on joint research areas (perhaps focused on improved risk models for third parties and suppliers), and active solicitation of input and guidance by the ratings companies of their provider customers on improved features, new products, and new services.[16]

Some questions we recommend security ratings companies consider in the context of improving their interactions with provider stakeholders include the following:

1. Are you able to actively collaborate with providers to collect feedback and verify actions taken to improve risk rating?
2. How often do you update the information used to calculate the ratings score assigned to a provider?
3. Which of the following additional elements are embedded in your analysis to produce a comprehensive risk score: Internal vulnerabilities, internal risks, external vulnerabilities, external risks, cloud security risks, third-party vulnerabilities and risks, and human risk?

Action Plan for ISPs and Vendors

The obvious broad recommendation is that ISPs and cybersecurity ratings companies must work more closely together – and this is not an issue for a specific vendor, but rather an industry-wide observation. It was repeatedly noticed during the interviews that providers rarely differentiated between the algorithms used by different vendors. This implies that the industry should work together on a more cooperative solution as per the USTelecom blog referenced above.[17]

Additional work between the providers and ratings companies might be coordinated at an industry level by organizations such as USTelecom or other cooperatives designed to encourage and enable information sharing. The TAG Infosphere team remains committed to help both the ratings companies and providers through its existing research and advisory services. It should be expected that excellent solutions become available and hopefully deployed in 2024.

The good news is that initial communications with top cybersecurity ratings providers in the industry has already led to progress. For example, two providers, Bitsight and SecurityScorecard, removed their industry scores for telecommunications firms from their public-facing websites after concerns were expressed about their accuracy by the industry. FortifyData has also provided useful input to the review process.

ABOUT USTELECOM

USTelecom is the national trade association representing network providers, innovators, suppliers, and manufacturers connecting the world through the power of broadband.

ABOUT TAG

TAG Infosphere is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises.

ENDNOTES

1 https://www.etno.eu/library/443-cyber-security-rating-a-rising-challenge-for-eu-industries.html

2 https://ustelecom.org/enhancing-cybersecurity-scoring-methodologies-a-call-for-improved-accuracy/

3 https://www.glasslewis.com/issuer-data-report/

4 The authors of this report, both having decades of experience in telecommunications cybersecurity, represent USTelecom, a trade industry organization that supports telecommunications-related businesses in the United States and TAG Infosphere, a New York City-based research and advisory firm founded by telecommunications veterans to support major initiatives including in cybersecurity.

5 Telecommunications participants in the research included AT&T, Verizon, Lumen, and T-Mobile. Cybersecurity ratings companies who participated in the research included SecurityScorecard and BitSight.

6 DMARC, which stands for Domain-based Message Authentication, Reporting & Conformance, is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email. See https://dmarc.org/.

7 https://www.sec.gov/news/press-release/2023-139.

8 A blog from US Telecom (see https://www.ustelecom.org/enhancing-cybersecurity-scoring-methodologies-a-call-for-improved-accuracy/) summarizes these concerns and helped to serve as a base for this analysis.

9 Readers desiring more information on the interview process are welcome to reach out to this primary author at eamoroso@tag-cyber.com. The discussions were held informally over video conference or phone and were designed to collect insight into their concerns with ratings in general, versus any concern with a specific vendor. While no formal contractual non-disclosure paperwork was involved in the discussions, existing relationships between this primary author (former CISO at AT&T for two decades) and the designates served as the basis for an informal agreement that the aggregated information would be included in this report but without any specific attribution or even casual inference to the sharing executive. Any errors or omissions in this report are entirely the responsibility of the author – and all designations here should be viewed as the author's personal opinion versus having any direct or indirect impact or indication of an individual ISP's views in terms of their contracts or other agreements with any or all cybersecurity ratings vendors.

10 The authors fully acknowledge that while security ratings companies certainly do have differing business models, sufficient business model similarities exist that most telecommunications firms and ISPs tended to not differentiate between the different vendors—*for the most part.* Obviously, the recommendations listed here regarding business models for security ratings companies must be instantiated and interpreted in the context of each individual vendor.

11 We are unaware of any non-profit security ratings organizations, which is obviously consistent with other types of ratings firms such as for financial creditworthiness. Security ratings companies operate as for-profit entities, often funded for high growth by venture capital firms.

12 See https://www.nist.gov/cyberframework/framework for more information on this important U.S. government model and how it drives a maturity-based approach to cyber risk quantification.

13 Readers interested in the analysis are welcome to solicit the authors for guidance on how maturity models and security ratings algorithms compare and contrast. In short, maturity-based risk models are frameworks used to assess the cybersecurity capabilities of an entity and its readiness to mitigate potential threats. Maturity models often utilize various stages or levels, each representing a higher level of cybersecurity maturity, to gauge an entity's progress over time. These models help entities understand their current cybersecurity posture and set realistic goals for enhancing their overall resilience. Maturity models do not provide specific risk scores. In contrast, cybersecurity risk ratings are typically quantitative assessments that assign a numerical or qualitative value (i.e., risk score or rating) to the level of risk associated with specific assets, systems, or vulnerabilities within an organization. Maturity models and risk ratings serve different purposes but can complement each other in a comprehensive cybersecurity risk management strategy.

14 The American Registry for Internet Numbers, Ltd. (ARIN) is one of five Regional Internet Registries (RIR) that serves the global Internet community by distributing and managing Internet number resources (IPv4, IPv6, and Autonomous System Numbers). The RIRs are referred to collectively as the Number Resource Organization (NRO), whose mandate is to actively contribute to an open, stable, and secure Internet. On their public website (which is where we derive the above description), ARIN openly acknowledges the challenges that they must deal with on an on-going basis regarding fraud and abuse. See https://www.arin.net/about/relations/law_enforcement/faq/.

15 A reverse DNS lookup involves searching for IP addresses using domain names.

16 As part of the research reported in this work, several sessions were coordinated between providers and ratings vendors to share views and solicit feedback.

17 One of the authors from TAG serves as an industry analyst, and under such work, has existing paid contractual research and advisory relationships with virtually all of the cybersecurity ratings vendors and a large number of domestic ISPs. This on-going work involves formal agreements for the author and his team at TAG Infosphere to respond to research inquiries, share technical and business insights, and work various projects at the request of the vendor or ISP, sometimes with great time-urgency for the customer. In virtually every case of the existing relationships, this topic of cybersecurity ratings for ISPs has emerged as a request and concern. It was first raised during ISP support at TAG during 2016 through 2021, and really increased in intensity during 2022 and 2023, especially as ratings began to increase in their representation in government filings.