FitchRatings

Exploring Bank Cybersecurity Risk

Better Insights into Growing Risk with Cybersecurity Scores from SecurityScorecard

Exploring Bank Cybersecurity Risk

Better Insights into Growing Risk with Cybersecurity Scores from SecurityScorecard

Fitch Ratings has worked with SecurityScorecard, a leading cybersecurity risk assessment company, and reviewed SecurityScorecard scores to gain insights into banks' cyber risk management. SecurityScorecard scores entities on their cyber risk health, using non-intrusive (outside-in) assessments. Cybersecurity scores show relative vulnerability to a cyber event and can provide valuable insight into cybersecurity risk.

Related Research

No Immediate Impact on Desjardins' Ratings as a Result of Data Breach (December 2020)

Financial Institutions Face Growing Cyber Risk Ratings Pressure (December 2019)

No Immediate Impact to Capital One's Ratings from Data Security Incident (July 2019)

ESG Factors Influencing Financial Institution Ratings (May 2019)

Introducing ESG Relevance Scores for Financial Institutions (February 2019)

Cybersecurity an Increasing Focus for Financial Institutions (April 2017)

Analysts

Christopher Wolfe
+1 212 908 0771
christopher.wolfe@fitchratings.com

Konstantin Yakimovich
+44 20 3530 1789
konstantin.yakimovich@fitchratings.com

Gerry Glombicki
+1 312 606 2354
gerry.glombicki@fitchratings.com

George Tsiantos
+44 20 3530 1796
george.tsiantos@fitchratings.com

Cybersecurity Risk is a Growing Threat

According to a recent McAfee Corp. report, the global cost of cybercrime topped USD 1 trillion in 2020, up almost 50% from 2018. The proliferation of reported and unreported attacks continues to increase at an alarming rate for several reasons including the potential for a financial payout, increased availability of tools to commit cybercrime, limited criminal enforcement to date, and a growing digital footprint. Attacks are becoming more sophisticated, not least due to the involvement of well-funded organized crime groups and nation-state actors.

The most recent IBM/Ponemon "Cost of a Data Breach" study showed that the average cost of a breach of fewer than 100,000 records was USD 3.86 million and a mega breach, one of over 50 million records, was USD 392 million. The study also indicated that the global financial sector took 177 days to identify a breach and another 56 days to contain the breach.

The trend of going digital was accelerated with COVID-19. The additional access points create more potential vulnerabilities, which in turn underscore the need for more robust monitoring and countermeasures.

Impact on Credit Rating Analysis

Cybersecurity risk has been a growing "non-financial" risk for banks over the years, typically occupying one of the top risks for many financial firms. High-profile data breaches including those at several of the largest and most sophisticated banks serve as sobering reminders of this ever-present risk factor. While cybersecurity risk often falls under the rubric of non-financial risk, there is a very real and growing financial impact that requires investment to mitigate risks and costs associated with fines, direct breach costs, reputational damage, supply chain interruptions, and lost business when a breach occurs.

Cybersecurity risk is a subset of the Risk Controls and Risk Appetite component of Fitch's Bank Rating Criteria. A material cyber breach would represent an event risk that could have rating implications, and while to date Fitch has not downgraded a bank solely in response to a cybersecurity event, cyber breaches have resulted in specific rating sensitivities for banks after they have occurred. While a cybersecurity event due to, for example, poor controls, can have negative rating impact, good cyber hygiene and strong controls are less likely to impact the ratings positively.

Key Findings from Review

- Banks with higher credit ratings typically exhibited better cybersecurity scores than banks with lower credit ratings.
- Developed market (DM) banks scored higher with less variability vs. emerging market (EM) banks. However, some EM banks exhibited good cybersecurity scores.
- Financial size does not necessarily lead to better cybersecurity scores.

Methodology

For the purposes of this research, we looked at 484 banks to which Fitch assigns both a Long-Term Issuer Default Rating (IDR) and a Viability Rating (VR), which reflects our view on a bank's standalone strength. The sample consisted of highest-level rated legal entities within banking groups. Subsidiary banks and banks with Long-Term IDRs driven purely by potential support were not included. The aggregate asset size of our sample was USD111 trillion and represented approximately 70% of global banking assets.

The observations below are based on point-in-time cybersecurity scores as of March 4, 2021 provided by SecurityScorecard for top-level web domains associated with our bank sample.

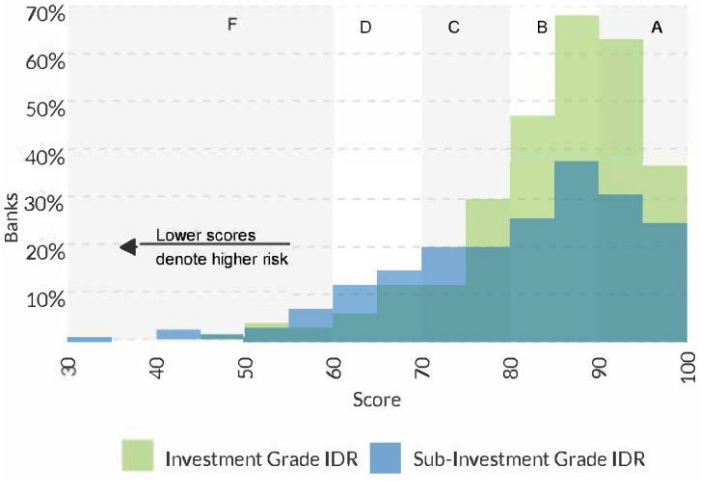
SecurityScorecard's scores range from 0 (highest risk) to 100 (lowest risk). Scores correspond to five cybersecurity grades: 'A' (best, corresponding to scores above 90), 'B' (80-89), 'C' (70-79), 'D' (60-69) and 'F' (below 60).

What SecurityScorecard Scores Reveal

Higher-Rated Banks Typically Exhibit Better Cybersecurity Scores

Our analysis of SecurityScorecard's scores for our sample revealed that banks with investment-grade credit ratings typically have higher (better) cybersecurity scores than their sub-investment grade counterparts. Higher rated banks in our sample also exhibited less variability around the scores.

Cybersecurity Score Distribution



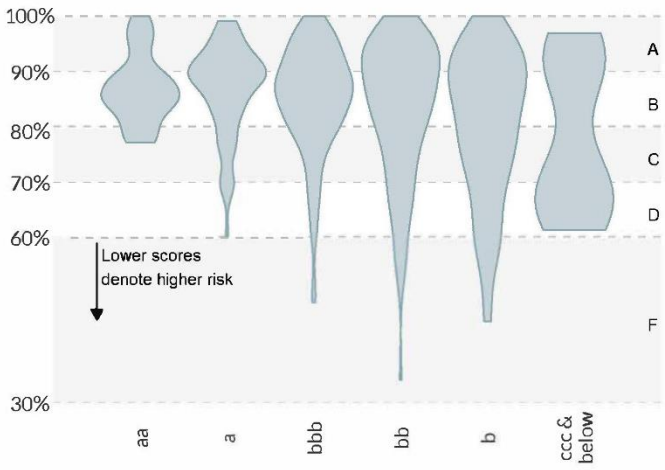
Source: Fitch Ratings, SecurityScorecard.

For example, for banks with a 'b' category VR, the variance of cybersecurity scores is almost three times higher than for banks with an 'a' category VR.

The fact that there is some positive correlation (~25%) between credit ratings and cybersecurity scores reflects the fact that a bank's operational risk controls have been a consideration for bank credit ratings, and the strength of controls is likely to affect a bank's cybersecurity risk posture. In addition, it may also reflect differences in banks' operating environments as higher-rated banks tend to operate in highly developed markets, which tend to benefit from a strong regulatory environment and supervisory oversight, possibly forcing banks to adopt more advanced cybersecurity risk management frameworks and adhere to stricter practices.

With that said, the data also shows that a high credit rating alone does not automatically mean that a bank will have a good cybersecurity score per SecurityScorecard's assessment. We found banks with scores corresponding to the two lowest SecurityScorecard cybersecurity grades ('D' and 'F') among all but 'aa' rated entities.

Cybersecurity Score by VR Category



Source: Fitch Ratings, SecurityScorecard.

Domicile Matters: Scores are Higher and Less Volatile in DMs

Our analysis shows that regional differences between banks' cybersecurity scores can be significant. Banks domiciled in DMs are typically scored higher with lower variability. About 80% of DM

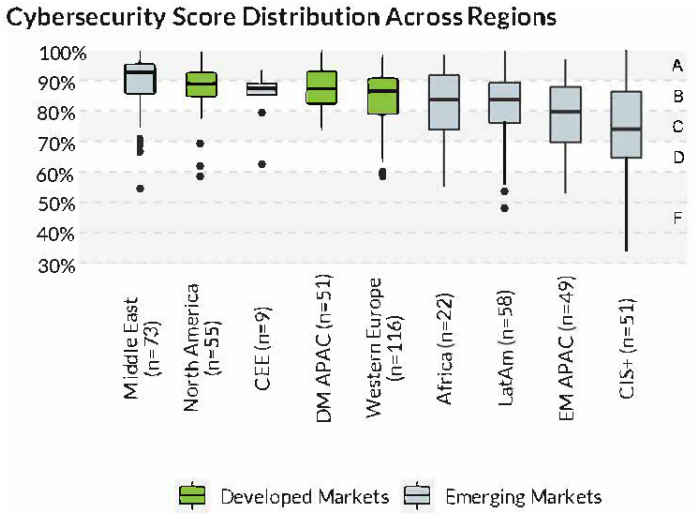
Cybersecurity Score by Domicile

Source: Fitch Ratings, SecurityScorecard.

banks in our sample scored in the top-two grades ('A' and 'B') on SecurityScorecard's scale compared to just 60% of EM banks. North American and DM APAC banks generally score slightly higher than banks in Western Europe.

We found that lowly scored banks can be present in DM countries and scores within a DM country can vary greatly. Banks subject to the same regulations and supervision can have significantly different cyber hygiene, leading us to believe that stronger regulations are a necessary but not sufficient condition for better cybersecurity scores.

In Western Europe, banks under profitability pressure in countries that suffered from banking crises (e.g. Italy and Greece) also have relatively lower cybersecurity scores, possibly as they may not have been able to invest in cybersecurity at the same rate as the broader industry.



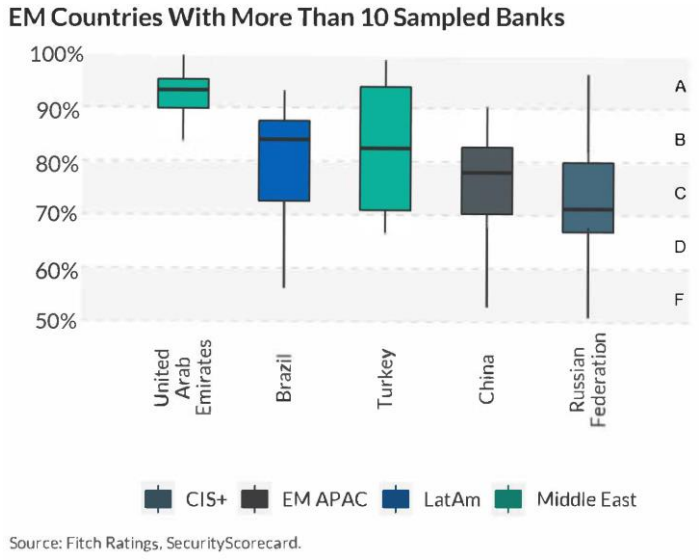
Source: Fitch Ratings, SecurityScorecard.

Not all EM Banks are Equal

However, the lower level of cybersecurity scores and the higher variability seen in EMs are not uniform. The Middle East is a notable example of an EM region where banks nevertheless scored highly. Together with banks based in North America and DM APAC, banks in the Middle East have on average the highest scores globally. They also have the tightest score distribution, with only a small number of entities scoring below the top-two grades on SecurityScorecard's scale. This could be attributed to high geopolitical tensions in the region for many years, which may have been a strong incentive for Middle Eastern banks to bolster their cyber risk posture.

Cybersecurity scores of Central and Eastern European (CEE) banks may be benefitting from EU rules and regulations and from the significant presence in these markets of Western European banks (which tend to score better). Other EM regions (Africa, EM APAC, LatAm and CIS, Georgia and Ukraine) consist of a large number of heterogeneous geographically spread markets, which may explain higher score variability.

Even though EM banks typically exhibited weaker cybersecurity scores, the rapidly evolving nature of technology and cyber risk does not mean EM banks will be at a long-term disadvantage on



Source: Fitch Ratings, SecurityScorecard.

cyber. In fact, EM banks could potentially close the gap with DM banks as they progress faster in their digital transformation, provided this transition is well governed, executed and controlled.

Size is not Necessarily an Advantage for Cybersecurity Risk

Intuitively, larger banks would seem to have an advantage in cybersecurity risk given their larger technology budgets, which can run to billions of dollars per year. However, our analysis of cybersecurity scores reveals that size is not necessarily a good predictor of cyber hygiene. In fact, we did not observe a correlation between a bank's size as measured by total assets or total operating income and a bank's cybersecurity score in our sample, with correlation remaining below 10% across the sampled portfolio.

There can be a number of factors that explain why financial size in and of itself may not be an advantage in cyber. First, a bigger and more complex bank is likely to have a larger digital footprint and hence a larger "attack surface". Larger banks are more likely to have complex and also legacy IT infrastructure compared to smaller banks, which could increase cybersecurity risk if not properly managed. Lastly, larger banks are more likely to be active internationally and as already noted, a bank's country or regional footprint could affect its cybersecurity risk posture.

Smaller banks may have newer and/or less complex IT infrastructure, which may have technology benefits for easier protection, benefitting their cybersecurity scores. Conversely, it may be more difficult for some smaller banks to attract appropriate talent or to invest sufficiently in cyber risk security, particularly when they do not have a strong regulatory incentive to do so.

Why Cybersecurity Risk Matters – Examples of Recent Attacks

The list of attacks presented below demonstrates that no entity is immune to a cyber-attack and the potential material impacts – reputational and financial, including remediation costs – of successful breaches. The list is not meant to be exhaustive and is based on publicly disclosed successful attacks on financial services companies that resulted in a financial cost of more than USD10 million, loss of data of more than one million customers or outage of a critical service for at least one day.

Date	Country	Company	What	Cost (if disclosed)	Impact
9/20	Chile	Banco del Estado de Chile	Ransomware attack		Nationwide closure of branches for one day
8/20	New Zealand	New Zealand's Exchange	DDoS attack (ransom)		Four-day outage of trading with intermittent availability
8/20	South Africa	Experian South Africa	Data breach		Personal information of up to 24m individuals and 800k businesses affected
7/20	US	'Dave' banking app	Data breach		Personal information, encrypted social security numbers and hashed passwords of 7.5m users leaked
5/20	Norway	Norfund	Data breach/theft	USD10m	$10m stolen via a fraudlent loan, likely following business email compromise
3/20	UK	Finastra	Ransomware attack		Partial outage over several days affecting client banks, particularly in North America
12/19	UK	Travelex	Ransomware attack	GBP25m	Outage of more than a month, cost is an estimate
12/19	Iran	Country's three largest banks	Data breach		Details of 15m debit cards leaked
11/19	Canada	Desjardins Group	Data breach	CAD108m	All 4.2 mil. member accounts affected
7/19	US and Canada	Capital One	Data breach	USD145m	Over 100m records affected, cost includes USD80m penalty
5/19	US	First American Financial Corp.	Data breach		885m files containing personally identifiable informaiton exposed; in Jul 2020 the regulator filed charges seeking penalties
3/19	Kuwait	Undisclosed bank	Theft	USD49m	
2/19	Malta	Bank of Valletta	Attempted theft		Attempted theft of EUR13m; one-day shutdown of services
10/18	Mauritius	State Bank of Mauritius	Theft	USD14m	Via fraudulent SWIFT messages following a breach; $10m subsequently recovered
8/18	India	Cosmos Bank	Theft	USD14m	ATM cash-out and fraudulent SWIFT messages; ATMs and online banking services suspended
5/18	Chile	Banco de Chile	Theft	USD10m	Via fraudulent SWIFT transactions, with a disruptive malware attack as a distraction
10/17	Taiwan	Far Eastern International Bank	Theft	USD14m	Via fraudulent SWIFT transactions, with a ransomware attack as a distraction
9/17	US	Equifax	Data breach	USD700m	148m accounts affected
11/16	UK	Tesco Bank	Theft	GBP18.7m	Via vulnerabilities in card issuance processes; GBP16.4m regulatory fine
8/14	US	JPMorgan Chase	Data breach		83m accounts affected, 1,000 hired for data security

Source: Fitch Ratings, Carnegie Endowment for International Peace.

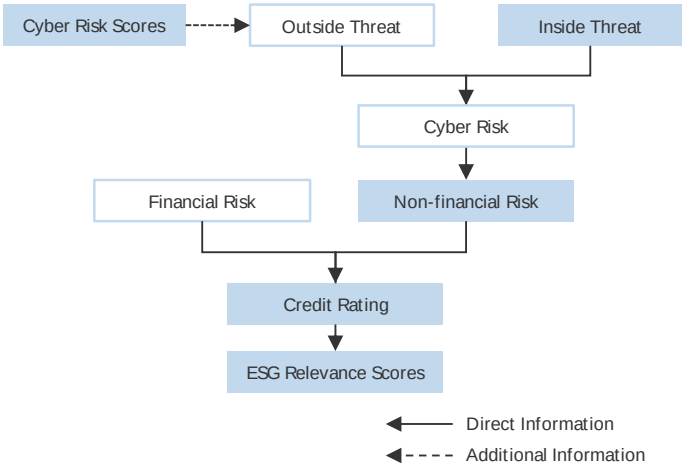
Cybersecurity Scores Can Inform Credit Ratings and ESG Factors

Cybersecurity scores offer a valuable insight into a growing risk. The 'outside-in' methodology used by SecurityScorecard offers a standardized way of looking at a complex risk area using a transparent methodology. A high cybersecurity score does not mean a company cannot be penetrated, just as a low cybersecurity score does not mean a company will necessarily be breached. However, low cybersecurity scores may help spot vulnerabilities at rated banks and raise questions about their cybersecurity risk management.

Cybersecurity scores offer a helpful additional data point that can complement and enhance the analysis of banks' risk controls and exposure to operational risk and allow analysis to be proactive rather than reactive. The availability of an independent third-party assessment, including scores, score components and their changes over time should also help deepen the conversation with banks on cybersecurity risk topics. The continuous and evolving nature of cybersecurity risk means that just because a bank demonstrates good cybersecurity hygiene today does not guarantee that this will remain true in the future. Conversely, those with weak cybersecurity scores today may see their scores improve over time.

In that regard, cybersecurity scores can serve to inform our view of cybersecurity risk generally, which in turn is a major element of event risk facing banks and other entities. For example, a stark discrepancy between a rating level and a cybersecurity score (for example, an 'F' grade for a bank rated in the 'a' or 'aa' range) is likely

Cyber Risk in Bank Criteria



Source: Fitch Ratings.

to draw analysts' attention and propel them to seek to better understand what drives the low grade and whether it should impact analysts' view on the bank's risk controls. Similarly, high volatility or a steady downward trend of a cybersecurity score for a given bank will likely prompt additional questions about the management of cybersecurity risk.

While Fitch has not downgraded a bank solely on the basis of cybersecurity risk, cybersecurity risk has been a noted rating sensitivity for banks that suffered a breach. Cybersecurity risk is also reflected in our ESG relevance scores, which are observations on ESG elements in the credit rating. Cybersecurity risk is typically captured as part of Social – Customer Welfare, Product Safety, Data Security, but could also be captured in Governance – Operational Execution or Governance – Governance Structure, to the extent a cybersecurity event had a nexus to a governance failing. Banks that experience cybersecurity breaches may see elevated ESG scores depending on the severity of the breach.

Next Steps

Fitch is keen to reflect operational risk weaknesses in our ratings as early as possible. Fitch will continue to study SecurityScorecard's data and how these can inform our analysis of an institution's cybersecurity vulnerability and plans to publish further insights based on cybersecurity scores such as the evolution of scores over time or impact of digital footprints on scores.

Moreover, we intend to explore the expansion of cybersecurity scores to other sectors, for example other financial services and corporates. We welcome feedback on our cybersecurity initiative at cyber.risk@fitchratings.com.

Appendix 1 — Key Developments in Bank Cybersecurity Risk Management

Banks often use or are subject to multiple frameworks that add complexity and cost. They may be subject to multiple regulatory authorities as well. Banks' cybersecurity risk frameworks are often an amalgamation of several regulatory, industry, and specific objectives. Appendix 3 contains a small sample of more prominent cybersecurity risk frameworks. The fact that there are many different frameworks, policies, and regulations speaks to the emerging nature of cybersecurity risk and attempts to manage cybersecurity risk.

Within larger organizations, cybersecurity risk is often managed by a Chief Information Security Officer (CISO). A CISO is a company executive responsible for an organization's data and cybersecurity needs. CISO's roles have grown in importance over the past several years and is even required by some regulations. A growing trend is for boards of directors to have a separate cyber risk committee with members who are experts in cybersecurity risk.

It is generally accepted that cybersecurity risk is best managed with an in-depth strategy that is routinely tested. Maintaining such a system is costly and time consuming; therefore, larger institutions tend to have an advantage over smaller peers given the ability to spread the cost over a larger base. However, larger institutions have more users and entry points, which create more vulnerabilities.

Institutions routinely employ third-party cybersecurity vendors that have expertise to bolster cybersecurity framework. However, involvement of third-party managers does not absolve a bank of cybersecurity risk and adds supply chain risk that needs to be managed.

Growing Role of Regulations and Regulators

Legislators, regulators, and supervisors continue to play an evolving role in establishing minimum levels of cyber hygiene. At the international level, the G7 issued Fundamental Elements of Cybersecurity for the financial sector, to consider issuing guidelines to achieve convergence on information and communications technology (ICT) risk. And the Committee on Payments and Market Infrastructures (CPMI) issued, jointly with the International Organization of Securities Commissions (IOSCO), guidance on cyber-resilience for financial market infrastructures (FMIs). Positively, international bodies such as the Financial Stability Board, Committee on Payments and Market Infrastructure, and Basel Committee have begun to strengthen coordination and foster convergence.

It is clear that, going forward, regulators, law enforcement, and banks must work together to create a globally effective risk mitigation standard that is a strong deterrent for cyber-related financial crime, yet is cost effective for institutions to implement and maintain. An example of significant cybersecurity regulation is the New York State Banking Department's 23 NYCRR 500, which requires minimum cybersecurity risk policies. The General Data Protection Regulation (GDPR) in the European Union is an example of a regulation aimed at protecting consumer data that also provides incentives to strengthen cybersecurity controls given significant potential fines in case of a data breach. Appendix 3 contains links to the full regulations for both. Cybersecurity risk frameworks and regulations are evolving, and greater convergence would add to banks' resilience.

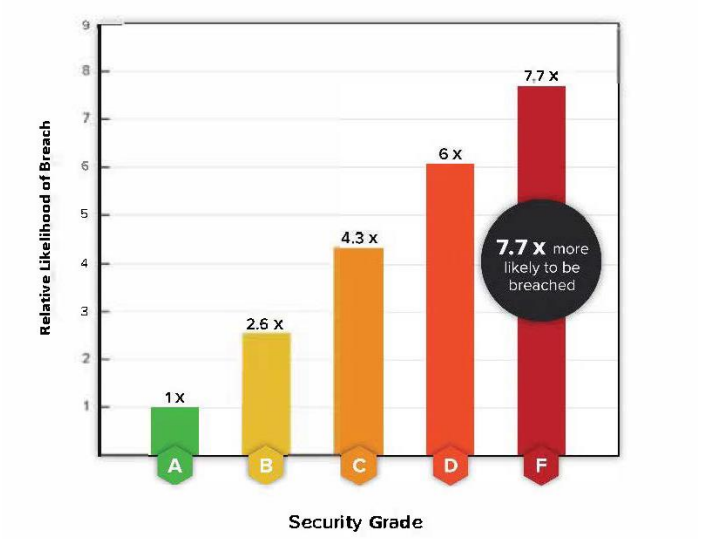
Appendix 2 — SecurityScorecard

Who is SecurityScorecard

SecurityScorecard is a leading cybersecurity risk assessment firm that provides a holistic "outside-in" view of an entity's cyber hygiene. It enables companies worldwide to understand potential challenges to their systems due to cyber risk in a transparent way with continuous cybersecurity scores. With easy-to-understand 'A' to 'F' grades, SecurityScorecard measures the cybersecurity posture of any organization in the world from an outside point of view that mimics a hacker's approach.

Cybersecurity scores can in certain ways be compared to financial credit ratings — just as a poor credit rating is associated with a greater probability of default, entities with an 'F' have experienced a 7.7x higher frequency of breaches compared to entities with a grade of 'A'.

Companies with a Better SecurityScorecard Grade are More Resilient



As with credit ratings, these scores are not a guarantee that a company with an 'A' grade will not be breached or that a company with an 'F' grade will be breached. Rather, they measure the relative likelihood of such a breach given a score.

It is important to note that cybersecurity scores are updated daily and can fluctuate materially due to an ever-changing threat landscape. New security vulnerabilities, minor changes in configuration, and new exploits can occur as often as daily. As a result, SecurityScorecard monitors changes on a daily basis for over 4.5 million scorecards and updates scores accordingly. It is unlikely to see significant grade adjustments in a short period of time absent a data breach. However, there are many cases where SecurityScorecard will detect a continued decline happening several months prior to a reported breach.

In addition to providing these scores, SecurityScorecard provides organizations with details on how these scores were derived and with to easily identify and prioritize risks for assessment and remediation, ultimately leading to a more secure environment.

SecurityScorecard Methodology

SecurityScorecard non-intrusively collects data by regularly scanning publicly available feeds across the internet for known vulnerabilities, outdated software, malware infections, and other relevant signals. With this information, SecurityScorecard attributes findings to legal entities, such as companies, governments, and non-profits, and then calculates a score that captures the cybersecurity risk of those organizations.

The data is used to calculate scores across 10 key risk factor groups that feed into a simple A to F grade:

SecurityScorecard's scoring methodology calculates a grade based on an organization's global digital footprint and observed security findings. Additionally, each security finding is marked as high, medium, or low severity based on the potential risk it poses to organizations, enabling users to understand which issues to prioritize for remediation. In order to eliminate scoring bias, SecurityScorecard compares the number of findings a company has to organizations with similar-sized digital footprints. This enables fair comparisons of an organization's cybersecurity hygiene against others of comparable size and brings increased accuracy, transparency, and fairness to the security scoring process.

SecurityScorecard utilizes both active and passive data collection methods to gather proprietary and third-party data.

Active data collection involves:

- Initiating a connection towards remote hosts and participating in some initial part of their protocol.

Passive data collection can be performed in two ways:

- A remote host connects to SecurityScorecard.
- Copies or summaries of some protocol transaction from a network sensor or intermediary device.

SecurityScorecard's proprietary data collection relies on a global network of sensors that examine the entire internet and identify services, vulnerabilities, and adherence to best practices, which can indicate a company's current cybersecurity posture. These signals are the fundamental backbone of an organization's security score. SecurityScorecard also operates a large network of sinkholes and honeypots to glean indications of malware infection from outside a company's network.

SecurityScorecard further enriches their data set by leveraging commercial and open-source intelligence feeds. This allows SecurityScorecard to improve the cadence of observation, build fidelity in the signals, and confirm accuracy in observations. All of SecurityScorecard's data collection methods use externally accessible and publicly-available data. No intrusive techniques are used to gather information.

SecurityScorecard identifies all the external-facing discoverable assets of an organization, the issues associated with those assets, and the severity of the threats that were found in order to determine a score for each organization. Additionally, the scoring algorithm is based on a statistical framework that considers the 4,500,000+ scored companies on the SecurityScorecard platform.

SecurityScorecard's scoring model is a continuous measure of the typical number of findings for an organization in relation to their size. The score is developed based on the number of standard deviations on which an organization is better or worse than the average number of findings for an organization of a particular size.

SecurityScorecard has fully documented and made public its scoring methodology and formulas. For further details on how SecurityScorecard creates these cybersecurity grades, visit the SecurityScorecard Trust Portal.

Limitations of Cybersecurity Scores

While cybersecurity scores can provide valuable insights into relative vulnerability to a cybersecurity event, this is still a nascent area of analysis, and the data sets only go back about five-seven years.

A key limitation of cybersecurity scores is the attribution of Internet Protocol (IP) addresses to a top-level domain. SecurityScorecard's attribution engine aims to programmatically capture the entire digital footprint of a particular domain (i.e. all IP addresses associated with it). According to SecurityScorecard, despite a rigorous process, it estimates a "false positive rate" of IP attribution typically less than 5%. Large banking groups are also likely to have a high number of domains associated with them, particularly when they have a high number of international subsidiaries.

The use of an "outside-in" methodology would not pick up the risk of an insider perpetrating an attack, as was the case with Desjardins Group. Insiders may have privileged access, intimate knowledge of the systems, including detection, and have a higher likelihood of successfully colluding to circumvent a control.

SecurityScorecard's cybersecurity scores do not speak to the financial impact of a cybersecurity event. They indicate the relative vulnerability but do not quantify the potential damage.

Appendix 3 – Key Cybersecurity Risk Resource

Broad-based frameworks for cybersecurity risk management:

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001

National Institute of Standards and Technology (NIST) Cybersecurity Framework.

Information Systems Audit and Control Association Control Objectives for Information and Related Technologies (ISACA COBIT).

Regulations related to cybersecurity risk and/or privacy:

European Union General Data Protection Regulation (EU GDPR)

New York Department of Financial Services Cyber Regulation

External Cybersecurity Research:

IBM/Ponemon Cost of Data Breach Report

McAffee "The Hidden Costs of Cybercrime"