BITSIGHT
The Standard in SECURITY RATINGS

A GLOBAL REPORT | Q1 2019

The BitSight Cyber Risk Monitor

IN THIS REPORT:
Managing Disruptive Risk

Managing Disruptive Risk

TOM TURNER
CEO & President, BitSight

Modern organizations are undergoing a digital transformation. Not unlike previous transitions, the shift from the traditional data center to the cloud presents both tremendous business opportunity – and significant risk.

Digital transformation, though, represents just one area of disruption. Emerging technologies, cybersecurity, and global topics such as political volatility, the economy, and even climate change are impacting today's businesses – often in unexpected ways. Consider the effects of a natural disaster, for instance.

In this unsettled environment, business leaders must think more broadly about the key risks their organizations face. Risk oversight must go beyond the enterprise-centric strategic, financial, and operational risks and also consider the atypical, disruptive risks.

This edition of the *BitSight Cyber Risk Monitor* offers thought-provoking perspective on how executives and corporate directors can approach the management of disruptive risk effectively.

In our Director's Corner, James Lam offers five recommendations for how corporate directors can incorporate disruptive risks into their risk oversight. He also discusses critical aspects of better governance that include constant surveillance, business alignment, and a focus on business resilience through risk mitigation and transfer of risk.

Our interview with cyber risk management advisor David X. Martin highlights his advice for board members, including the increased importance of internal due diligence and managing third-party risk.

Finally, key BitSight Analytics provide practical industry benchmarks and trends in cybersecurity program performance and compromised systems – vital baselines that serve to inform boards in their decisions on how to review cybersecurity program performance, prioritize risks, assess third parties, and focus their resources.

Just as risks evolve, so too must organizations in how they manage them. The problem with disruption is that often, organizations are not prepared for it. Or there are biases for how it should be managed. Or their tools are not configured – or effective – for a digital world.

It's time to think differently. Use the information in these pages to start talking about and preparing for the unexpected. And consider that disruption not only carries risk, but also opportunity. How you approach the oversight of this disruption can mean the difference between being disrupted – or taking control of the outcome.

On behalf of the team at BitSight, I thank you for your continued engagement and for being part of the evolving conversation that is focused at the intersection of business and cyber risk.

Sincerely,

Tom Turner
CEO & President, BitSight

Director's Corner

JAMES LAM is president of James Lam & Associates, a risk management consulting firm. He also is a director of E*TRADE Financial, where he chairs the risk oversight committee, and a director of RiskLens, Inc. The National Association of Corporate Directors [NACD] recognized him as one of "the most influential directors" in the NACD Directorship 100 in 2017 and 2018. He is certified by the Software Engineering Institute of Carnegie Mellon in Cybersecurity Oversight.

Board Oversight of Disruptive Risks

Disruptive risks represent one of the hottest topics for corporate directors. On a global basis, we face disruptions in critical areas such as geopolitical volatility, economic slowdown, emerging technologies, cybersecurity threats and climate change.

While disruptive risks are top concern for directors, their confidence in corporate risk management is alarmingly low. In a recent NACD poll, 62% of directors viewed disruptive risks as "much more important" than five years ago, however, only 19% of directors expressed confidence in management's ability to address such risks. Given the current business environment, we need to close that gap.

Disruptive risks are threats that are existential to an organization. Their impact may be sudden or occur over a number of years.

An animal metaphor of black swans, gray rhinos, and white elephants can be useful in defining the three main types of disruptive risks:

- **Black swans** are "unknown unknowns" or highly improbable events that are difficult to predict. Examples include the 9/11 attack and the 2008 financial crisis.
- **Gray rhinos** are "known unknowns" or observable trends that often are ignored. Examples include artificial intelligence and cybersecurity.
- **White elephants** are "known knowns" or significant issues that are extant but difficult to acknowledge and manage. Examples include irrational CEO behavior and sexual harassment cases that ushered in the #MeToo movement.

How should directors incorporate these disruptive risks into their risk oversight?

Following are my **top five recommendations** for consideration. Cybersecurity, one of the most critical disruptive risks, is highlighted as an example.

1. **Incorporate disruptive risks into the board agenda**
   The full board should discuss the potential impact of disruptive risks, including the effect on business strategies, financial returns, and long-term enterprise value.

   For cybersecurity, the full board should evaluate risk/return trade-offs between digital opportunities and inherent cyber risks. Furthermore, the risk committee should determine cyber risk policies and risk appetite statements while the audit committee should provide additional oversight with respect to independent testing of internal controls.

2. **Ensure enterprise risk management (ERM) practices are effective**
An ERM program is critical to support board oversight of disruptive risks. Fundamental ERM tools used for enterprise risks – risk assessments, key risk indicators, risk tolerances, and dashboard reporting – can be applied to disruptive risks.

   One of the key principles of ERM is to consider interdependencies across risks. Board oversight of cybersecurity should include the critical interdependencies between cyber risk management and third-party vendor oversight, data governance, business contingency planning, and other operational risk processes.

3. **Consider scenario planning and analysis**
Directors should recognize that disruptive risks often are atypical threats with no historical precedent or loss data. Scenario analysis, a forward-looking approach, can be a valuable tool to evaluate the consequences of a full range of potential outcomes.

   For cybersecurity, this would include tabletop exercises or scenario-based war room simulations. These exercises should evaluate multi-vector attacks, disruption of normal communication channels, and critical incident response and board escalation requirements.

4. **Ensure board-level risk metrics and reports are effective**
A unique aspect of disruptive risks is that they are often fraught with subjectivity. Moreover, cognitive biases – such as optimism, group-think, and status quo – can get in the way. Independent and objective data are useful antidotes.

   Objective cyber risk metrics include independent security ratings, penetration test results, and phishing test results. Ideally, these metrics are benchmarked against other organizations based on industry, region, or competitive peer group.

5. **Focus on resilience**
The financial and reputational fallout from disruptive risks can be sudden and severe. One of the key objectives for the board is to ensure the organization can continue to carry out its core business functions.

   Companies cannot always prevent a cybersecurity breach, but they can enhance business resilience by investing in detection controls, risk mitigation, and business recovery. The board should also review the company's crisis management and communication plans, as well as loss coverage through corporate insurance or self-insurance.

As directors, we need to think more broadly and deeply about the key risks our organizations face. Our risk oversight must go beyond well-defined strategic, financial, and operational risks and consider atypical, disruptive risks. We need to address the existential risks that can be characterized as black swans, gray rhinos, and white elephants.

An Interview with a CRO

OUR INTERVIEWEE:

DAVID X. MARTIN is a cyber risk management advisor to business leaders and corporate boards. He also provides expert witness testimony in cases involving cyber security breaches and risk management. His 40-year career as a senior financial executive includes senior positions at PwC, Citibank, and AllianceBernstein. Visit DavidXMartin.com or email dxm@davidxmartin.com to learn more.

Q **You were Chief Risk Officer (CRO) at several major financial institutions. What is the role of the CRO with respect to understanding and overseeing newer, disruptive risks such as cyber?**

A The best CROs are the glue that ensures that all of the organization's risks are being managed. CROs need to become more integral in the management cybersecurity by: providing oversight from a strategic business perspective, creating an effective constructive challenge function, and ensuring that cybersecurity is integrated effectively into enterprise risk.

Q **As a board member, how do I get comfortable with my organization's approach to cyber risk management?**

A If your organization has a strong cyber-immune system, you can feel reasonably confident that your company is thinking about cybersecurity in the right way and taking appropriate steps to protect the enterprise. Analogous to the human immune system, which mounts a three-step defense, a cybersecurity defense would:

- Sound the alarm. Constant surveillance is critical, with early warning indicators and multiple layers of defense.
- Solve the problem. Manage cyber security at the enterprise level and not treat it as "just a technology issue."
- Recover and remember. When things go wrong, the ability to identify and respond to a problem quickly will determine your company's ultimate recovery.

Your organization's cyber-resilience program must bring together the areas of information security, business continuity, and organizational resilience.

Q **What does active risk management in cybersecurity look like?**

A The traditional approach to security relies on prevention strategies. In contrast, an active intelligence-driven mindset is based on the assumption that the company already has been compromised and, therefore, must evolve continuously to stay ahead of the curve.

Critical to this "active" approach are accurate threat modeling, a quantifiable asset valuation, and "what if" scenarios that consider the deterrence factors of a security measure or process, as well as their cost. The right intelligence-driven approach is based on prior experiences, current threat intelligence, an understanding of breaches that have impacted other companies, trends, valuation of assets, and an analysis of the safeguards to guard these assets constantly, including when controls fail.

OUR INTERVIEWER:

JACOB OLCOTT is Vice President of Communications and Government Affairs at BitSight. He speaks and writes about the role of directors, officers, and executives in cyber-risk management. His paper, "The Board's Role in Cybersecurity," was published in 2014 by the Conference Board. He is a member of the Conference Board's Cyber Governance Advisory Group, and served as Cybersecurity Attorney to the Senate Commerce Committee and House Homeland Security Committee.

Q **Many organizations are experiencing cyber incidents as a result of a vendor's insecurity. What are the best practices regarding third-party due diligence?**

A A third-party vendor program should include: the awareness of third-party exposures prioritized based on risk (including cyber) to the organization, a set of in-place clear assessment tools for the on-boarding of any new relationships, in-place and continuous risk-adjusted monitoring processes to assess the third-party's adherence to contract terms, external third-party assessments of vendor practices, and joint disaster recovery testing with primary service providers.

A strong third-party vendor management program does more than strengthen cybersecurity risk management. It can support spending decisions, contracting strategies, service levels, and other critical operational activities to support the attainment of the organization's core business objectives.

Q **What should the board rely on with respect to its own due diligence?**

A The board should understand the full range of cyber risks that its organization faces and encourage management to develop appropriate strategies tailored to the company's specific needs and business goals.

Any effective cyber program includes careful planning, smart delegation, and a system for monitoring compliance – all of which directors should own. Smart network surveillance, early warning indicators, multiple layers of defense, and learning from past events are all vital components of true cyber resilience.

When things go wrong, whether in a major or minor way, the ability to identify and respond quickly to a problem will determine the company's ultimate recovery. Cybersecurity cannot be guaranteed, but a timely and appropriate reaction can.

BitSight Analytics

Security Ratings increase transparency about cybersecurity, enabling dynamic, informed interactions among global market participants and incentivizing a more secure global ecosystem.

Providing Data-Driven Context

The broad measurements, continuous monitoring, and data-driven objectivity of standardized metrics such as BitSight Security Ratings are vital baselines that serve to inform business leaders in their decisions on how to review cybersecurity program performance, prioritize risks, assess third parties, and focus their resources.

BitSight Analytics taps into the more than 210,000 companies in our inventory, 120+ data sources to reference, and ownership of the world's largest sinkhole to gain important ongoing measures and assessments of how companies across multiple industries and regions are performing with regard to cybersecurity.

BitSight Security Ratings

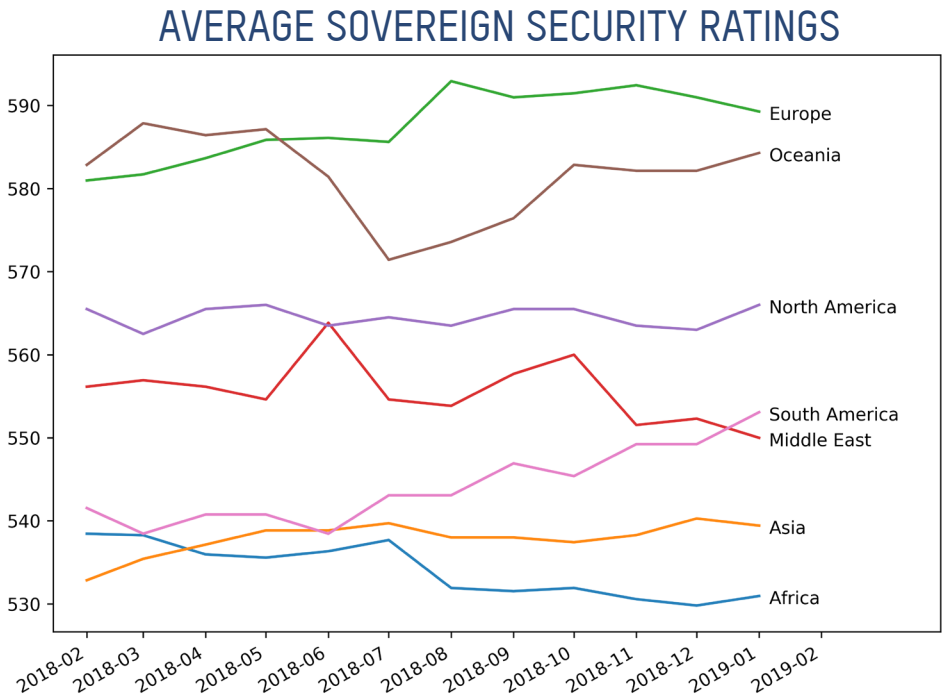
BitSight Security Ratings apply sophisticated algorithms to produce daily security ratings in three categories, including Basic (250-639), Intermediate (640-739), and Advanced (740-900). Lowest to highest, these ratings are a quantitative measure of an organization's existing security posture. The charts on pages 9-10 reflect BitSight Security Ratings by industry. The median rating, reflected on each chart by a "★" is that industry's "standard of care."

Sovereign Security Ratings

Sovereign Security Ratings are an objective and unbiased measure of relative security performance. The charts on page 8 reflect BitSight Average Sovereign Security Ratings at the country level and at the industry level. They are calculated on a scale of 250-900 with higher ratings indicative of better security.

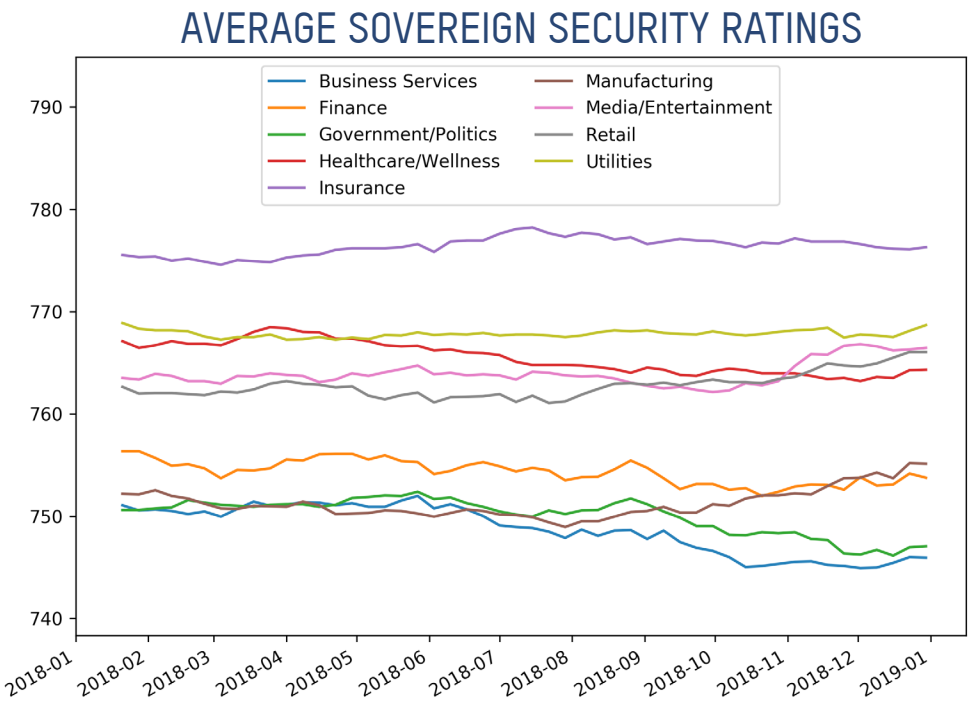
MEASUREMENT OF RELATIVE SECURITY PERFORMANCE

BY REGION



MEASUREMENT OF RELATIVE SECURITY PERFORMANCE

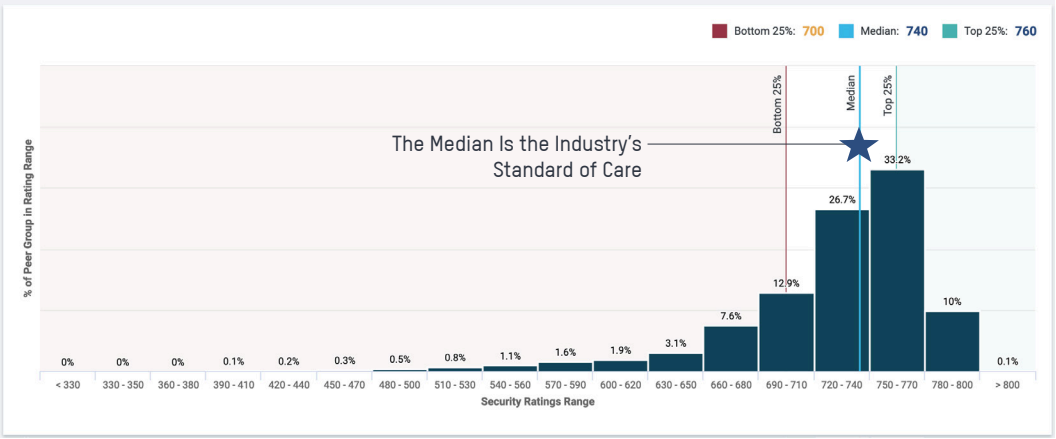
BY INDUSTRY



BUSINESS SERVICES

MEDIAN RATING:

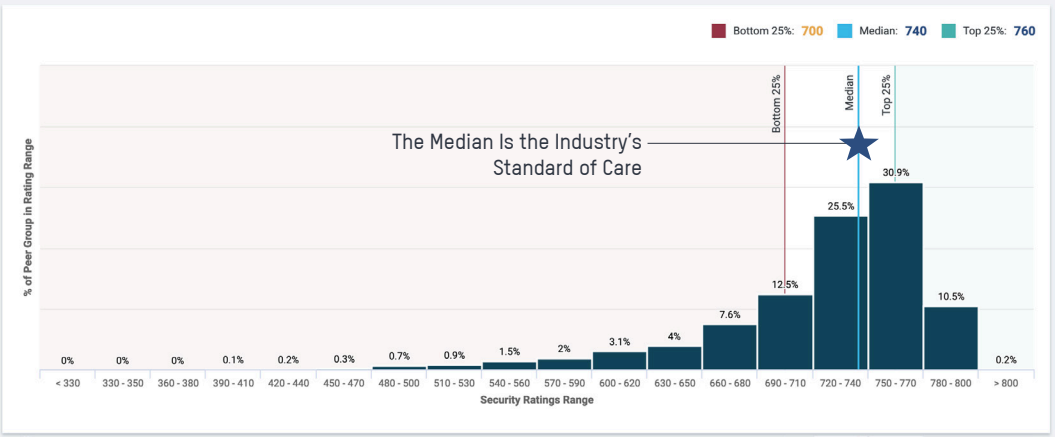
740 ADVANCED



HEALTHCARE

MEDIAN RATING:

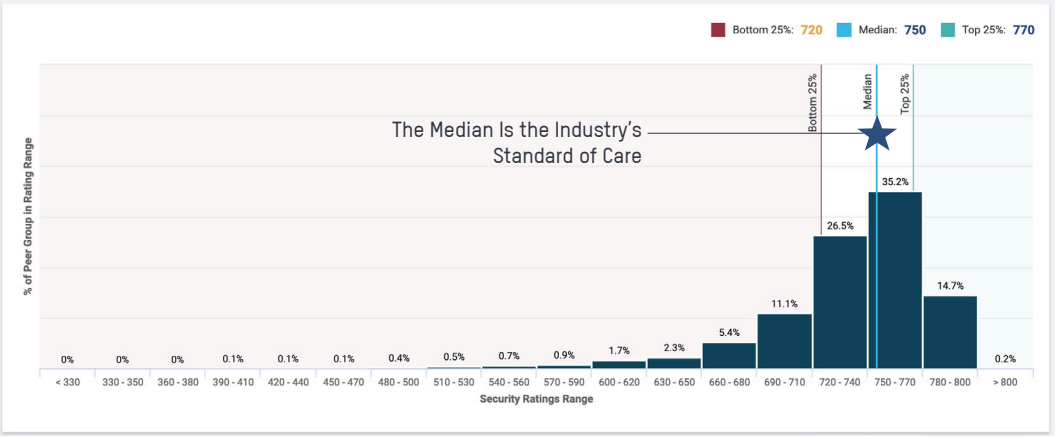
740 ADVANCED



INSURANCE

MEDIAN RATING:

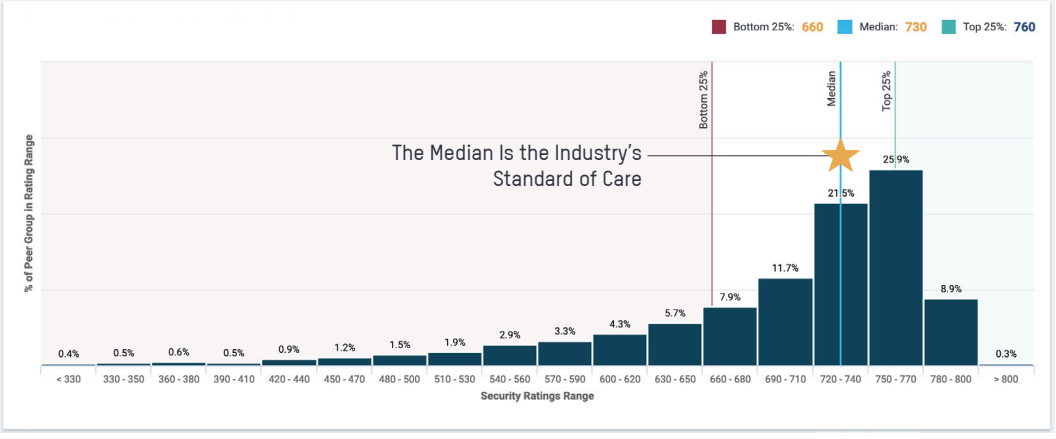
750 ADVANCED



GOVERNMENT

MEDIAN RATING:

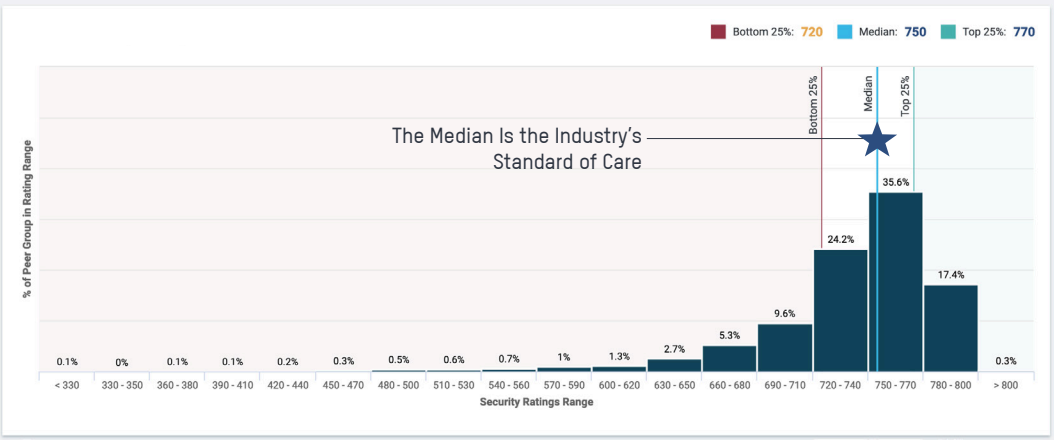
730 INTERMEDIATE



FINANCE

MEDIAN RATING:

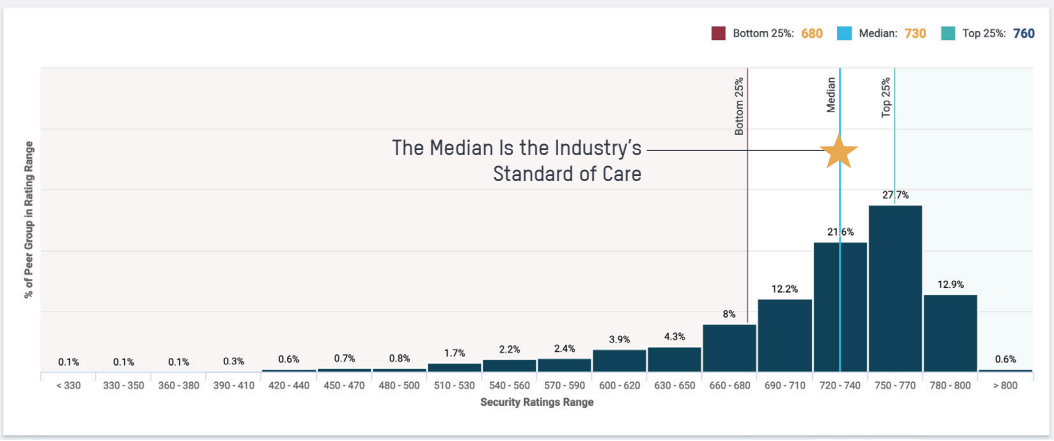
750 ADVANCED



RETAIL

MEDIAN RATING:

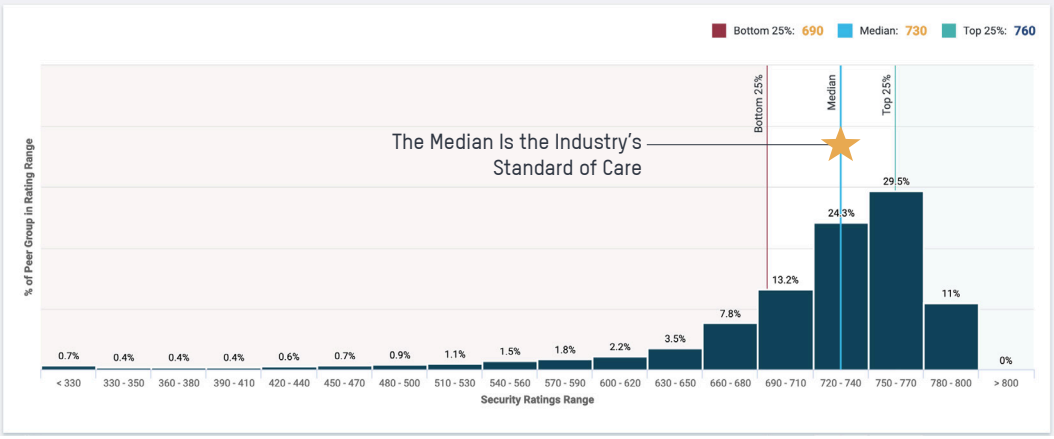
730 INTERMEDIATE



TECHNOLOGY

MEDIAN RATING:

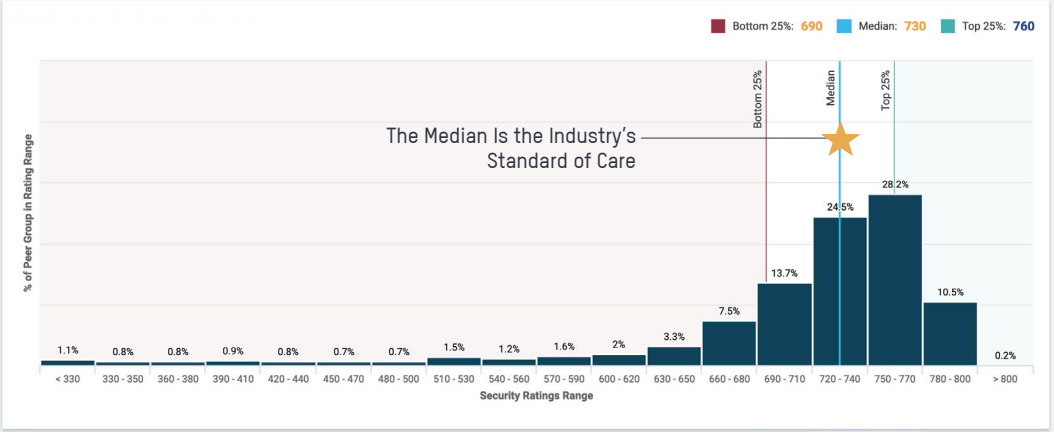
730 INTERMEDIATE



UTILITIES

MEDIAN RATING:

730 INTERMEDIATE



Better Data.
Better Decisions.

Subscribe to the **BitSight Cyber Risk Monitor** for important insights into the global cyber risk landscape.

www.BitSight.com/directors

BITSIGHT®
The Standard in SECURITY RATINGS

BitSight
111 Huntington Avenue
Suite 2010
Boston MA 02199
+1.617.245.0469

About BitSight

BitSight transforms how organizations manage information cybersecurity risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of data on security issues. Seven of the top 10 largest cyber insurers, 20 percent of Fortune 500 companies, and four out of the top five investment banks rely on BitSight to manage cyber risks. For more information, please visit www.BitSight.com, read our blog or follow @BitSight on Twitter.