BITSIGHT
The Standard in SECURITY RATINGS

EBOOK

A Practical Guide to Risk-Based Cybersecurity Reporting

INTRODUCTION

There's no question about it: Today's cybersecurity landscape is evolving faster than ever. From the ongoing migration to the cloud to the widespread shift to remote work, there are a variety of factors causing your enterprise's attack surface to expand rapidly — exposing you to new and changing cyber risks, while making it increasingly difficult to gain continuous, broad visibility into your critical assets. At the same time, you're being tasked to meet the shifting expectations of your role with increasingly limited time and resources.

As budgets decrease and teams continue to adapt to our "new normal" operating environment, it's more important than ever to have a strong strategy in place for assessing, monitoring, and reporting on cyber risk and security program performance over time.

After all, some of the most devastating data breaches in history have occurred when security alerts and warnings were ignored. The Equifax hack could have been avoided if a security technician hadn't overlooked an email requesting a critical security patch. The SEC did nothing with years of urgent recommendations to encrypt sensitive financial data that would go on to be breached. The Home Depot breach of 56 million payment card numbers was attributed to managers who repeatedly ignored warnings from staff that security wasn't strict enough. (The managers responded, according to the New York Times, "we sell hammers.")

And now, cyber attacks are on the rise as malicious actors are taking advantage of the potential flaws in our new operating environment to advance their nefarious objectives. According to a recently conducted study by the Information Systems Security Association (ISSA) and Enterprise Strategy Group (ESG), cybersecurity professionals saw a 63% increase in cyber attacks related to the COVID-19 pandemic.

Effective communication between different levels of a cybersecurity organization — from practitioners to managers to the C-suite and the Board — can mean the difference between secure systems and massive incidents. And reports, far from being a formality or busy work, are the central mechanism of this communication.

By taking a risk-based approach to cybersecurity reporting, you can assess performance based on actual exposure to cyber threats, provide actionable context, highlight the value of your cybersecurity efforts, and ensure you're getting the most out of your limited time and resources.

In this ebook, we'll take a look at the importance of cybersecurity reporting — and the techniques, software, and methodologies that are revolutionizing the reporting process at every level of the organization.

REPORTS VS. ALERTS

An important distinction: When we refer to reports, we're talking about collections of data and insights compiled by people, not the alerts automatically generated by software tools.

Automatic alerts, though hugely valuable, cannot be substituted for real interpersonal communication. Firstly, there are simply too many alerts to take them all seriously. In a 2018 Imperva survey, 55% of IT professionals reported receiving more than 10,000 threats daily — while 27% noted more than one million.

Secondly, alerts generated by machines are too easy to dismiss without a human to understand them, translate them into non technical language, and use them to advocate for actionable change. In the Imperva survey, 53% of respondents indicated that, amongst all the noise, their organization's Security Operations Center (SOC) has struggled to pinpoint which security incidents are critical. To make matters more complex, the SOC is stretched more thinly than ever before — with many teams having to tackle additional functions, such as remote support, in our "new normal" operating environment.

In many cases, alerts on their own are insufficient. In order to take the alerts and convert them into actionable reporting, security teams must assess the context and have direction on how to separate the signal from the noise.

WHAT IS RISK-BASED REPORTING?

The contents of cybersecurity reports are highly variable, and depend on the nature of the report, its creator, and its intended recipient. However there are certain factors that can be used to determine whether any cybersecurity report is effective:

- Does the report convey actionable information in context?
- Is the report concise enough that key findings don't get buried?
- Is the language in the report clear enough for a non-technical audience to understand?
- Does the report relate findings back to cyber risk?

When organizations lack meaningful internal reporting about cybersecurity, it can typically be attributed to a failure to meet one or more of the criteria listed above.

Reports that provide numbers without insights or context are more likely to be overlooked, especially if the reader doesn't have the skills or knowledge to draw conclusions from the data. Reports that contain too much information or information that's too technical can cause frustration, leading readers to wish they had "a handheld translator, the kind they use in Star Trek," as one top executive put it.

Among these components, the last — does the report relate findings back to cyber risk? — may be the most important. This question forms the basis of a risk-based reporting approach.

Risk-based cybersecurity reporting, as opposed to comprehensive, compliance-based, or incident-based reporting, is the approach best suited to reducing an organization's actual exposure to cyber threats. Following a risk-based approach to cybersecurity reporting can help individuals and teams at all levels of an organization focus on the most significant issues without falling victim to alert fatigue and ignored warnings.

Reports that provide numbers without insights or context are more likely to be overlooked, especially if the reader doesn't have the skills or knowledge to draw conclusions from the data.

What Does Risk-Based Cybersecurity Reporting Look Like?

There are many ways to practice risk-based reporting, but the following recommendations can help your organization get there.

- Place the highest-risk items front and center in the report.
- Assign a "risk score" to key findings or recommendations.
- Put findings in context by comparing metrics to past performance, peers, and competitors.
- Frame risk in business terms to help executives and leaders understand the ramifications of findings.
- Report on critical items frequently, or implement continuous reporting dashboards.

CONTEXT CLUES

Metrics presented in a vacuum are rarely actionable. What does it mean, for example, that your firewall has stopped 1,500 intrusions this month? Is that a lot, or a little?

A risk-based cybersecurity report delivers findings in context, helping the recipient understand what role a number plays in the overall risk landscape of the organization. This context may include any of the following:

Past performance: What were these same numbers like last month, or last quarter? Are you improving or getting worse over time?

Risk concentration: How are different business units and subsidiaries across your organization performing?

Industry benchmarks: How does your performance compare to your peers and competitors?

Financial quantification: What's at stake financially with your current risk posture?

Cybersecurity frameworks: How do your findings align to cybersecurity frameworks for your industry — such as the NIST Framework for Improving Critical Infrastructure Security, CIS Critical Security Controls, ISO 27001, or PCI DSS?

With the appropriate context, practitioners, managers, executives, and Board members can all make more confident decisions about cybersecurity, assigning the appropriate resources to the projects most likely to reduce risk across the organization.

A risk-based cybersecurity report delivers findings in context, helping the recipient understand what role a number plays in the overall risk landscape of the organization.

RISK-BASED REPORTING FOR BOARD MEMBERS

Boards have become increasingly involved in cybersecurity oversight over the past decade. The start of this trend can be traced back to Target's 2013 data breach, after which an advisory firm recommended that seven of the ten board members be replaced for failing to adequately oversee cyber risk as part of their duties. This report signaled a major shift in corporate cybersecurity policy, with executives and Board members taking a much more hands-on role.

As the top-most link in the chain of cybersecurity reporting, Boards have a responsibility to create a culture in which each subsequent link — from executives to managers to practitioners — reports on information that is actionable and based on actual cyber risk.

Risk vs. Compliance

For Board members, it's imperative to understand the difference between cybersecurity as it pertains to compliance and cybersecurity as it pertains to actual cyber risk.

Boards, being answerable to regulators, have reason to be concerned about cybersecurity compliance. However, there is often a big difference between compliance and true security. Achieving compliance and achieving an acceptable level of risk are discrete goals, and should be treated as such.

To this end, Directors must ensure that CISOs' and CIOs' reports to the Board don't focus exclusively on compliance or risk, but rather track progress toward objectives in each of those areas.

Achieving compliance and achieving an acceptable level of risk are discrete goals, and should be treated as such.

Creating a Culture of Transparency

To operate effectively, Boards need a full picture of their organization's cyber risk — which in turn requires Board members to be able to trust the information coming from their cybersecurity executives.

Building this trust calls for Boards to focus on creating a culture in which no one is afraid to tell the truth about cybersecurity issues, even if that truth is potentially damaging, such as a human error that allowed a threat into a network or the failure of an individual to patch a certain program.

And, as the old saying goes, Boards must trust, but verify. While Boards don't typically have the time or expertise to verify individual data points, they can leverage continuous monitoring tools, like security ratings, to see at-a-glance whether the information coming up from their executives is reflecting the true, real-time state of cyber risk across the organization.

Questions Boards Should Be Asking About Cybersecurity

- What is the current state of cyber risk at the organization?
- What are the biggest gaps in our cybersecurity programs?
- What are we doing to close these gaps and mitigate cyber risk?
- Are we allocating resources based on risk level?
- Are we aware of important threats that are affecting our industry?
- Is our cybersecurity strategy aligned with our business strategy?
- If a cyber attack or data breach happens, are we prepared to respond?
- Are the responsibilities of cybersecurity personnel clearly articulated?

RISK-BASED REPORTING FOR EXECUTIVES

> *Boards and committees are swamped with reports, including dozens of key performance indicators and key risk indicators (KRIs). The reports are often poorly structured, however, with inconsistent and usually too-high levels of detail. Research indicates that most IT and security executives use manually compiled spreadsheets to report cyber risk data to their boards; unsurprisingly, many board members are dissatisfied with the reports they receive.*
>
> - Cyber Risk Measurement and the Holistic Cybersecurity Approach, McKinsey, 2018

In their reports to other executives and Boards of Directors, cybersecurity executives must do the difficult work of putting technical concepts in context for non-technical individuals.

Risk-based reporting provides a framework for accomplishing this. To answer the question “what does this mean?”, it’s not necessary for executives to educate their superiors on the technology underpinning a certain KPI. Instead, they must relate the finding back to cyber risk. For example: What does it mean that we have an above-average number of open ports? It means we’re at a 9% higher risk of experiencing a data breach than the average company in our industry.

Strategic Reporting

In addition to adding context and making reports less technical, security and risk executives can deliver more compelling presentations to the Board and other executives by including a strategic component.

Instead of reporting strictly on present cybersecurity posture, executives can increase the impact of reports by laying out a roadmap of their strategic vision. By including their short-, medium-, and long-term goals for the organization’s cybersecurity and putting cybersecurity metrics in the context of these goals, CIOs and CISOs can demonstrate the effectiveness of certain initiatives.

In addition, security and risk executives should aim to put their reports in the context of the overall business strategy. Cyber risk management should always be in alignment with an organization’s broader enterprise risk management framework. CFOs, CEOs, and Board members are going to take the information from a cybersecurity report and try to understand how it will impact their larger goals — execs can help this process along by reaching their own conclusions and including them in their reports.

Getting the Right Resources

One of the principal functions of cybersecurity reporting at this level is to help higher-ups with their budgeting and resource allocation decisions. For example, if a CISO is requesting a new technology solution to improve overall cybersecurity, a good Board will look to past reports as part of their due diligence process.

A common issue that arises in this process is the inability on the part of the cybersecurity department to prove the effectiveness of a given solution, whether it's a software program, a new hire, or some other initiative. This has historically been difficult — after all, aside from some complex KPIs that a Board may or may not understand, the only visible measure of the effectiveness of a cybersecurity solution is whether or not the organization falls victim to a cyber attack.

Risk-based reporting has the power to revolutionize this process. Using a solution like security ratings, executives can track changes in actual cyber risk against the timelines of certain solution implementations. For example, if your organization invested heavily in security awareness training and your malware rating went down significantly, that correlation can be used to ask the Board for further investment. This type of context and visibility is more important than ever as, according to BitSight data, up to 85% of the workforce in some industries shifted to remote work in March 2020. While this new operating environment opens the corporate network up to new vulnerabilities, it also requires a variety of new types of investments to be made to enable teams to work securely and efficiently at home.

Using a solution like security ratings, executives can track changes in actual cyber risk against the timelines of certain solution implementations.

KPIs Executives Can Use in Their Reports

CEOs and Board members often complain about the highly technical nature of cybersecurity KPIs. To combat this, executives can use KPIs like the following that are easy to understand or contain built-in context:

- Security rating
- Average vendor security rating over time
- Average industry security rating
- Intrusion attempts within a given period
- Patching cadence
- Mean time to detect
- Mean time to resolve
- Backup frequency
- Phishing test success rate
- Security awareness training scores

RISK-BASED REPORTING FOR MANAGERS

For managers, much of the work of risk-based reporting comes down to choosing the most relevant performance indicators.

Security and risk managers will each have different responsibilities depending on their specific roles and the size and structure of their organizations. However, they all share one critical responsibility: synthesizing information and reporting on it to upper management and executives.

Managers play a unique role. They're responsible for operationalizing the decisions made by leadership and allocating resources to execute strategy. In many organizations, managers might experience a disconnect between what they think their team needs and what their team has been given to work with.

Risk-based reporting can solve this issue. If a manager can understand the business impact that certain issues are having on the overall cyber risk of their organization and communicate this impact effectively, they can more closely align their superiors' understanding of the organization's cybersecurity with their own.

Picking and Choosing

A cybersecurity manager might have access to thousands of data points. Which they choose to report on can have an impact on the meaning they're able to convey up the chain. Choose to pass along too much or too little data (or data without context), and the lack of clear communication could lead to a major security incident like the breaches at the SEC and the Home Depot.

For managers, much of the work of risk-based reporting comes down to choosing the most relevant performance indicators. This is not a call to cherry-pick the data to meet an agenda, but rather to limit the amount of total indicators reported on in order to avoid inundating recipients, and relate the findings back to the larger context of company-wide goals, strategies, and KPIs.

How should a manager decide which indicators to include in their reports? Using a risk-based reporting methodology, the indicators that most closely correlate with actual cyber risk should take priority.

Continuous Reporting Using Dashboards

Curated reports are extremely important to ensuring that important information gets communicated to the right people. However, reporting is just one small entry on a long list of responsibilities for security and risk managers. Many managers will simply be too busy to compile thoughtful reports as often as they'd like.

Enter the dashboard. Many new cybersecurity solutions include integrations that allow them to continuously export certain data to dashboard software. Managers now have the option of curating a dashboard that upper management and executives can check whenever they'd like to get a quick picture of cybersecurity or risk. While building a dashboard, it's important for managers to remember the importance of context — dashboards should be aligned with KRIs and KPIs to maximize impact.

Equipped with this continuous reference tool, executives can make decisions that more closely consider actual conditions in the cybersecurity department.

Core Elements of a Risk-Based Cybersecurity Dashboard

Security rating: These synthesized measurements of an organization's cybersecurity performance are continually updated. Some security ratings have been independently proven to correlate with risk of data breach. Include an industry average or preset goal to add context to this rating.

Risk vector grades: Some security ratings platforms give users the ability to see grades on specific risk vectors, such as malware servers or patching cadence. These can be chosen based on their relevance to the specific function being reported.

Recent incidents: A feed of data from a SIEM can show executives how many and what kinds of threats are being detected in an organization's systems.

Threat intelligence: Which kinds of malware have been found in the organization's systems? Which threats are affecting the industry in general?

Security awareness training data: User-related risk is one of the least addressed risk areas in many organizations. Including data that illustrates the effectiveness of awareness training (completion rates, test scores, phishing test results, etc.) can help illustrate its importance.

RISK-BASED REPORTING FOR PRACTITIONERS

With BitSight Forecasting, you can identify the optimal course of action to improve your cybersecurity risk posture by modeling different scenarios and paths of remediation.

For the individuals charged with doing the actual hands-on work of mitigating cyber risk at an organization, daily life is a constant series of resource allocation decisions. And in our “new normal” operating environment, making these decisions can be more difficult than ever. After all, many cybersecurity professionals are taking on new responsibilities, such as general IT support, while being challenged to work with decreasing budgets. Having one’s time tied up with one project necessarily means an inability to work on another.

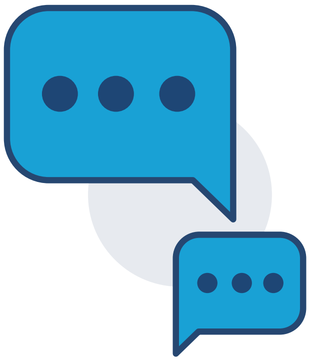
With limited personnel to perform all the necessary duties of keeping an organization safe from cyber threats, this is a high-stakes exercise. Working on protecting low-risk data while high-risk controls go unimplemented can lead to a massive incident.

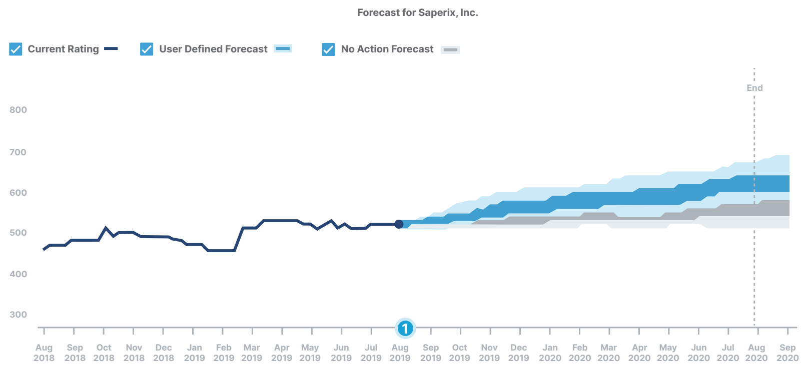
Unfortunately, it can be difficult for practitioners to demonstrate their own effectiveness. If a data breach occurs as a result of poor decision making on the part of a manager or executive, blame can too easily be passed down the chain. This is due to a divide between operational and strategic metrics — while a practitioner can report on which patches they applied or how many ports they closed, it’s difficult to say what impact those activities had on meeting cyber risk goals.

Forecasting Success

Practitioners can use risk-based reporting to demonstrate their effectiveness and assist their managers in deciding where their skills are most needed.

One of the best methods for risk-based reporting at the practitioner level is forecasting, a feature built into the BitSight for Security Performance Management platform. With BitSight Forecasting, you can identify the optimal course of action to improve your cybersecurity risk posture by modeling different scenarios and paths of remediation. Armed with these insights, it’s easier than ever to gain answers to difficult, but important questions about where to spend security budgets, which sets of activities will reduce risk most quickly, and whether technology implementations should be changed.





An example scenario: A practitioner has been leading a team that has been implementing controls to improve email security. A manager decides that their email systems are secure enough, and wants to use that team for other projects. The practitioner can then forecast a scenario in which certain email risk vectors (SPF, DKIM, etc.) are not implemented fully, and report on the simulated impact that scenario will have on the organization's overall security rating. Demonstrating that the impact will keep the organization from reaching its stated risk goals, the practitioner can successfully make the case that email security should remain a priority.

CONCLUSION

In a cyber risk landscape defined by high-profile breaches and constantly evolving threats, all types of organizations must take a hard look at the state of their internal communication. And now, as enterprises are working with an increasingly remote workforce, having clear, data-driven conversations around cyber risk has never been more important. The lessons have already been learned that poor communication can lead to devastating incidents — it's time for leaders to take those lessons to heart.

Risk-based cybersecurity reporting is the best mechanism for improving internal communication about cybersecurity. Furthermore, implementing this reporting approach at all levels of the organization is central to the development of truly effective security performance management strategy.

Get a risk-based look into your organization's cybersecurity.
Request your FREE Security Rating Snapshot.

GET STARTED

BITSIGHT®
The Standard in SECURITY RATINGS

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.