SPOTLIGHT

Sponsored by: DataBee from Comcast Technology Solutions

Possessing a cybersecurity intelligence-gathering capability is no longer a luxury but a critical need for a data-driven cybersecurity leader to be successful. Impactful insights from a contextual intelligence fabric can aid executives in objective and unbiased risk management decision-making.

Principles of Being a Data-Driven Cybersecurity Leader

October 2024

Written by: Philip D. Harris, CISSP, CCSK, Research Director, GRC Services and Software

Situation

Managing cybersecurity programs without intelligence and insights to accelerate decision-making is a huge challenge in today's rapidly evolving threat and regulatory landscapes. In the current environment, governance, risk, and compliance (GRC) platforms do very little in the way of presenting risk and compliance insights to enrich the context of issues discovered, such as identifying owners or classifying assets or data. Insights such as these would tremendously aid the analyst in prioritizing and mitigating issues and driving issues to closure sooner rather than later.

Historically, there has been a limited set of data metrics that provided minimal value in the overall oversight, risk, compliance, and operations of programs for cybersecurity leaders. For example, these metrics reported on noncompliance and whether compliance gaps were addressed, prioritized, or partially resolved. Some of these involved blocking threats or patching vulnerabilities, yet what was often presented to analysts was neither actionable nor a clear call to action. Metrics and statistics were often in multiple repositories and formats that required extensive time to reformat for usability. Compounding this limitation involved collecting the required metrics and statistics simply, easily, and centrally. The collecting of metrics was laborious, time-consuming, and almost never in the form necessary to present to executive management.

While these types of metrics aided in managing a tactical program, it was not enough information for the cybersecurity leader to think strategically and function as a business leader alongside the executives of the organization. These types of tactical metrics also made it difficult to mature cybersecurity programs to a strategic level. Metrics that create insights, aid executives in decision-making, and show an organization's risk posture are critical for cybersecurity leaders' success in today's fast-changing threat landscape and regulatory environment, and possessing a cybersecurity intelligence gathering platform will be key to achieving this success.

AT A GLANCE

WHAT'S IMPORTANT

Possessing a contextual cybersecurity intelligence-gathering capability is no longer a luxury but a critical need for the data-driven cybersecurity leader.

KEY TAKEAWAYS

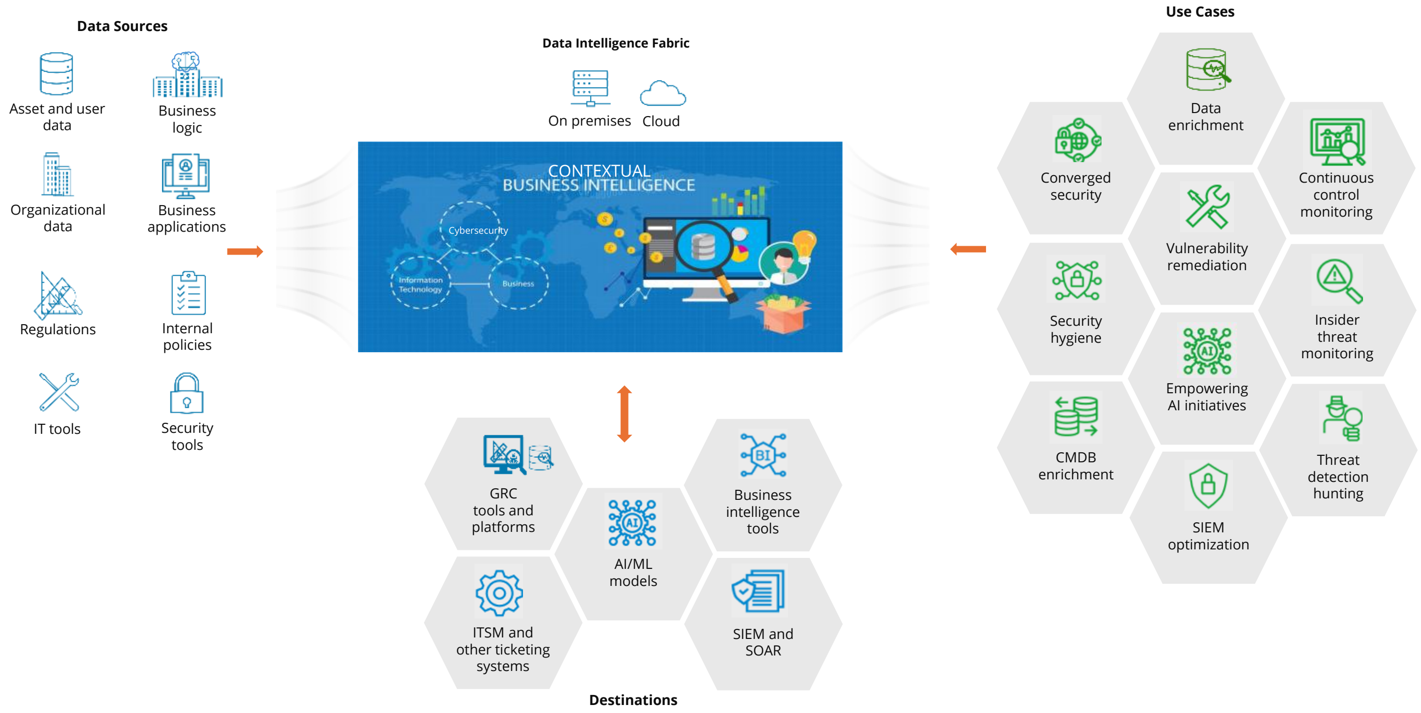
Business, IT, and cybersecurity data are significantly enriched by the collection of intelligence from data sources throughout the organization.

This intelligence is curated to create accurate, reliable, unbiased, and objective results for decision-making by executives, for critical risks that could mean the difference between a resilient organization and a vulnerable one.

What Is Needed?

Today's environment calls for a capability to collect rich contextual information from data sources that provide not only metrics and statistics but additional business, regulatory, IT, policy, risk, and compliance insights and themes from across the organization based upon use cases to aid in strategic management. In the current environment, various control systems such as GRC platforms can enhance their activities and findings utilizing a rich source of business and cybersecurity intelligence data to bring forth additional insights and derive key criteria such as data and asset ownership or classification. Figure 1 describes this contextual data intelligence repository (fabric) that is sourced from a variety of data sources throughout the business and IT estate collected into a single data intelligence repository (or fabric) specifically designed to broker intelligence between the data sources and the destination control systems to satisfy various business use cases deemed critical by the organization.

FIGURE 1: ***Contextual Cybersecurity Data Fabric***



Source: IDC, 2024

The fabric, as illustrated in Figure 1, is a separate collection of information that is distinct from the control data collected and used by the destination systems in Figure 1. The destination systems can then utilize the additional context provided by the fabric to derive additional insights or enhance features and functionality. In the case of GRC tools and platforms, the fabric will enrich and enhance the information in the GRC risk register to create additional context behind a risk or compliance issue. In addition, this advanced fabric can also contribute to the automation and orchestration of risk and compliance methodologies by providing information such as new assets discovered, the potential sensitivity of data and assets, the potential owners of data and assets, and the potential financial impact on the organization. The additional context also aids the analyst in interpreting risks and compliance issues against the policies for the organization.

The fabric enhances GRC platform capabilities that increase or accelerate the ability to collect and utilize outcome-driven and actionable contextual metrics, statistics, and insights. Examples of these are as follows:

- Centralization of the collection of relevant cybersecurity, IT, and business information that becomes the "source of truth" of all governance, risk, and compliance information and intelligence
- Collaboration with business, IT, and executive stakeholders
- Centralized dashboards that cater to specific stakeholders, as dashboards that are important for the security operations center would not communicate what is important to the executives and board members
- Outcome-driven and actionable metrics, statistics, trends, and risk-driven insights
- Stakeholder messaging types that accommodate both the audience and the type of audience reaction expected such as the following:
  - For your information only
  - Executive risk-based decision required
  - Budget being requested
- Significantly reduced human bias and increased accuracy

Principles of Data-Driven Decisions

Data-driven decisions elevate and enhance the cybersecurity leader and program to effectively manage cybersecurity as a strategic component of the overall business strategy. Discussions about risk and compliance issues and their impacts on business strategies become a normal and commonplace activity that engages stakeholders, makes issues clear, and renders risk and compliance decisions mindfully. This fabric is in the form of language that communicates risks such as likelihood versus impact to the business, whether financial or otherwise.

The key principles to help cybersecurity leaders transform into data-driven leaders include the following:

- **Understanding the risks:** Often, cybersecurity programs do not start with identifying the key or critical risks to the organization. This is an ongoing activity as the company and cybersecurity program evolve. Identifying key stakeholders from the business, IT, audit, legal, risk, and/or compliance officers; business information security officers; and senior executives can be a productive way to accomplish this. In addition, these stakeholders will need to agree on the prominent risks that could affect the organization, which will lead to buy-in. Armed with this information, it is possible to measure a cybersecurity program against these risks, especially when there is a fabric with cybersecurity intelligence capabilities that not only feeds information into a GRC platform but also collects a vast amount of contextual intelligence throughout the IT estate.
- **Aligning data collection and retention:** After identifying these risks, collect the relevant data associated with them. This may involve identifying data sources, identifying ways to automate the collection, and being prescriptive in retaining this data for specified periods of time defined by the business. Fortunately, many destination systems like GRC tools and platforms, business intelligence tools, SIEMs, or even ITSM and ticketing systems can utilize this kind

of contextual intelligence for a variety of reasons beyond cybersecurity including IT process management, IT metrics, and contribution to AI and ML models.

- **Analyzing the data:** Automation and AI can make use of contextual cybersecurity intelligence in combination with the risk register to analyze large volumes of data and produce results that aid in managing GRC use cases. This could also generate additional insights not uncovered in the past that illuminate or highlight evidence or justification to support outcomes. Ultimately, you are looking for patterns in the data that could illuminate risks and other adjacent insights such as lack of asset or device ownership and classification, which would otherwise go unnoticed and not contribute to the overall measure of risk.

- **Interpreting the results:** Tying data into decision-making is a key aspect of this principle. This is likely the most critical step in the process because a data-driven leader is looking for results that are outcome driven, actionable, and in alignment with the risks critical to the business. Outcomes are the result or impact of the cybersecurity program, services, controls, and projects. These are specific, measurable, and meaningful and are the events, occurrences, or changes in conditions or behavior or attitudes that indicate progress toward goals. Outcomes are what you hope to achieve when you meet the goal. For example, if a cybersecurity capability including technology, people, and processes is in place to address a key risk to the organization, then revealing the outcome will measure progression toward ensuring successful mitigation of the risks. An example is the implementation of a data loss prevention (DLP) solution, which should demonstrate that users are learning from their actions when DLP stops them, when data exfiltration is identified and reduced, and — most importantly — what the outstanding residual results are.

- **Considering the stakeholders:** A good practice is identifying which stakeholders need to understand the underlying metrics of the outcomes — especially the actionable outcomes that will impact them. Stakeholders are very busy people (like the cybersecurity leader), and it is important to communicate any outcomes that are pertinent to their organization including the risks associated with that organization. Different lines of business (LOBs) will likely have different risks to manage that are a subset of the overall risks posed to the organization. Focus the outcomes to generate a story about how these risks impact the business, what steps they need to take to manage these risks, and any other relevant actions that are necessary. For example, an LOB manager for manufacturing will likely not be interested in security system events that made it through to the network unless the manufacturing systems are connected to the network. However, if the manufacturing network is segmented from the greater corporate network, there may be less of a need to communicate actions necessary to address the risk. An LOB manager for the revenue-generating ecommerce environment will be interested in application security and the risks that improper application architecting or control implementation pose.

- **Empowering decision-making:** The principles behind decision-making — especially as they relate to the cybersecurity leader — are typically misunderstood. The cybersecurity leader does not own the decision-making for managing risks but does own recommending how to mitigate risks and communicating them to the stakeholders as well as the decisions — including actions and budget requirements — necessary to address those risks. The data-driven cybersecurity leader is responsible for creating an environment in which the decision owners are making informed decisions about risk that leverages connected data and contextual insights bringing clarity to the decision owner.

- **Monitoring and optimizing:** This series of steps constitutes not only the principles that are to be followed but also the principles that can be transitioned into a repeatable set of processes. Ongoing monitoring of the processes associated with these principles is necessary to ensure that all stakeholders and executives are continuously in alignment with the processes. For example, GRC teams can be more active participants because the data is easy to interpret, the progress is more easily monitored because the feedback loop is sustainable, and stakeholders are clearly labeled. There will be a need to continuously optimize various aspects of these processes. For example, there will be a need to revisit decisions around determining the risks to the business. As the program progresses, some areas of risk will be managed to the degree that these no longer significantly impact the business. Therefore, ongoing discussions about which risks the business should focus on will be necessary. This feedback loop allows for continuous improvement and learning from the data-driven decision-making process.
- **Establishing processes and guidelines:** Establish clear processes and guidelines for data access, security, and data governance to ensure that self-service data is balanced with appropriate controls. Seek executive support and create a community in which data-driven decision-making is valued and embraced at all levels of the organization. A data-driven decision-making culture takes time and effort, but the benefits of making informed choices based on evidence and insights are invaluable.

Benefits

- **Accuracy and reliability:** Decisions are based upon factual data and evidence within the system, allowing for the formation of original, objective, and insightful ideas rather than biased or subjective ideas, thus bringing greater clarity and accuracy to stakeholders where decisions are more reliable.
- **Objectivity and reduced biases:** Decision-making becomes more objective, and bias is significantly reduced in the results.
- **Insights and understanding:** Patterns that would otherwise go unnoticed begin to appear and provide valuable information tied to the decision-making process.
- **Opportunities and risks:** Risk evaluation becomes more objective and straightforward. Opportunities arise for spotting trends, gaps, and suspicious behaviors.
- **Planning:** Strategic planning and alignment with organizational goals is easier when data views are shared, making them more apparent and measurable.
- **Stakeholders:** Being data driven and consistent with outcomes and results causes stakeholders to become champions of the process.
- **Efficiencies and cost:** Data-driven decisions optimize efficiency by presenting and analyzing data that connects the business with historic trends. Businesses can streamline processes and — as a result — internal costs begin to lower.
- **Improvement and innovation:** Monitoring outcomes, gathering feedback, and analyzing data causes organizations to gradually learn and adapt.

- **Confident decisions:** As data becomes reliable and accurate, decisions become much easier to make because the facts are staring you in the face, so to speak.

Technology or Vendor Profile

DataBee from Comcast Technology Solutions (CTS) is a cloud-native security, risk, and compliance data fabric platform. Customers work smarter with an evidence-centric approach to security that prepares them for what is next. Developed on the foundations of a security data fabric, DataBee offers a continuous controls monitoring (CCM) solution that delivers connected security and compliance data and insights for the three lines of defense, providing the same data-driven views to bring clarity to roles and responsibilities.

Comcast Technology Solutions, a division of one of the world's largest global companies, Comcast Corp., owns the DataBee business. CTS is chartered with bringing Comcast's proven technologies to other large, regulated enterprises. Inspired by a platform created for use within Comcast Corp. and delivering such promising results — from cost savings to faster threat detection to compliance answers and more — DataBee is designed for scale. In 2022, Comcast executives funded a business around this emerging technology space and hired great talent from pure-play security and data technology companies to develop, sell, and operate DataBee, which today has over 120 professionals spanning all functions and serving clients across three continents and five countries.

Challenges

The challenge for Comcast's DataBee and adjacent capabilities will be to ensure that customers understand that the platform provides all the capabilities necessary to manage GRC programs using an underlying rich, contextual intelligence data fabric that sets it apart from today's traditional GRC platforms.

Conclusion

Managing cybersecurity programs without objective intelligence and insights that could accelerate decision-making is a huge challenge in today's rapidly evolving threat and regulatory landscapes. Cybersecurity leaders traditionally made decisions using a limited subset of metrics that were generalized, did not tell the complete risk story, and were minimally useful in the overall oversight, risk, compliance, and operations of the program. Metrics and statistics were often in multiple repositories and different formats requiring extensive time to reformat for usability. Compounding this limitation was the inability to collect the required metrics and statistics simply, easily, and centrally. This effort was laborious, time-consuming, and almost never in the right form to present to executive management.

While these types of metrics aided in managing a tactical program, they did not provide enough information for cybersecurity leaders to behave strategically and elevate themselves to function as business leaders alongside the executives of the organization. Contextual intelligence from throughout the IT estate that creates impactful insights, aids executives in objective decision-making, and shows the risk posture of an organization is critical for data-driven cybersecurity leaders. Possessing a cybersecurity intelligence-gathering capability is no longer a luxury but a critical need for a data-driven cybersecurity leader to be successful.

About the Analyst

***Philip D. Harris, CISSP, CCSK,** Research Director, GRC Services and Software*

Phil Harris is responsible for developing and socializing IDC's point of view on governance, risk, and compliance services and software across people, processes, and technologies focused on creating a foundation of privacy and trust with enterprises, IT suppliers, and service providers.

MESSAGE FROM THE SPONSOR

Data is the shared business language. It provides a North Star to inform leaders, empower teams and guide them towards their business objectives. Yet, too often, data remains scattered across an organization; the time and effort it takes to prepare and process data to extract insights — even with data scientists on staff who know how to extract meaning from data chaos — is daunting.

DataBee's executive KPI reporting capabilities make data that shared language, enabling CISOs, CIOs and GRC executives (among others) to more easily see how they are doing against their unique security and compliance KPIs and take action to mitigate risk and close compliance gaps. These reporting capabilities make it significantly easier for CISOs and CIOs to communicate with top executives and the Board how the organization is doing against its goals for managing risk.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
blogs.idc.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.