Brought to you by Informa Tech

Publication date:
07 Feb 2024
Author(s):
Curtis Franklin, Principal Analyst, Enterprise Security Management

On the Radar: CDW SPARQ provides risk management in a retail package

Summary

Catalyst

Enterprise security management rests on a foundation of risk quantification. Framing the story of that risk and the costs associated with managing it in front of executives and board members is a significant part of the cybersecurity manager's job. With Security Program Assessment and Risk Quantification (SPARQ), CDW has fielded a service that endeavors to put quantified enterprise cyber-risk on the table, surrounded by a story told in language that business executives and board members understand. SPARQ is a model for the kind of service that can add significant organizational maturity to the process of managing cybersecurity risk by involving the board and helping them prioritize risks and methods of dealing with them.

Omdia view

Successfully engaging the executive board in an appropriate conversation about risks and responses is always a challenge for cybersecurity managers, many of whom come from the practitioner ranks. Their instinct is often to address the issue with technical language and a highly tactical level of detail. What executives, and, in particular, boards of directors need for making decisions is information presented in business terms to address strategic questions.

CDW's SPARQ service quantifies risk based on input from a risk-quantification tool—X-Analytics—though the service can use other programs or frameworks as input if the customer is already committed to an existing risk-quantification tool or service. In this way, SPARQ can appeal to a wider variety of clients

because it does not force a company to change risk quantification tools if one is already in place. No matter which tool SPARQ gathers info from, quantified risk in the final presentation is expressed in terms of USD—the critical measurement of risk in a business context. Expressing risk in USD terms is important for moving the conversation about risk out of the cybersecurity group and into the broader business.

SPARQ makes quantified risk the center of a narrative that can be adapted for the intended audience, whether that audience is cybersecurity managers or an executive board. As a service, SPARQ can help the customer quantify cyber-risk in USD as a business sum, then work with the cybersecurity and corporate risk management departments to put that risk into context and prioritize the risks based on which ones could have the greatest business impact, which risks can be modified or transferred more cost-effectively, and which can be reasonably accepted. The CDW team can then coach the customer on building this information into a story that makes sense to executives or the corporate board in the effort to gain agreement with and approval for investment and action. With its aid to business prioritization, this story makes SPARQ a strong entry in the cybersecurity risk quantification segment of enterprise security management.

Why put CDW SPARQ on your radar?

CDW's SPARQ is a service intended for companies looking to increase their cybersecurity maturity and build on a quantitative basis for prioritizing security investments. It enables the chief information security officer (CISO) to evaluate how to reduce cyber-risk based on cyber-spending tradeoffs and expected risk reduction—quantified in USD. SPARQ is not unique in providing risk quantification, but it is quite special in the way that it puts the quantification in context and helps customers build an understandable, compelling story around the numbers.

SPARQ provides decision support to the CISO and other executives for resource allocation by offering the ability to model various risk scenarios and responses. The service provides tools to the CISO to perform risk and cybersecurity analysis using planned spending and expected cyber-risk reduction as the criteria. The results are summarized for presentation to executives (or the board of directors) using USD exposures instead of the qualitative cyber-risk descriptions that are typically provided.

The professionals who deliver the SPARQ service do not approach the data gathering, coaching, and presentation construction as an exercise in building a story for a single-budget cycle but rather as a step in a longer relationship in which the customer's security maturity will increase while the risk management and business expertise of the client's staff grow.

Market context

There is no question that risk quantification is now a required function in enterprise security management. In the 2023 Omdia Decision Maker Survey, only 8% of respondents said their companies use no-risk quantification tools. There also can be no question that cybersecurity has risen to a board-level concern, driven by the growing number of laws and regulations that make boards not only responsible for demonstrating organizational security competence but also liable for security breaches. The challenge for enterprise security managers has been to act effectively on the motivation generated by the two factors—legal/regulatory pressure and increased potential board liability—working together.

The irony is that there are tools and frameworks available to help enterprise security managers understand and act on quantified risk, but they have not seen broad acceptance due largely to the complexity and expense of using them effectively. For some time, enterprise security managers looking to put risk

quantities into forms and factors necessary for executive and board-level presentations have had limited choices in how to approach the challenge.

One common approach is to take the output from a risk quantification product or service and put it into a framework providing context. This generally means using a product such as Security Scorecard, MetricStream, or RiskLens to initially gather and quantify cyber-risk, then a framework such as NIST, ISO, or FAIR to put the risk into context. It is a process with a number of challenges, including the need to be at a relatively high level of security maturity to reasonably expect to complete the complex task of putting data into a framework.

The frameworks have been essential tools for giving context to risk, but they are not often able to provide guidance on prioritizing those risks or the investments to deal with them. With options for dealing with risk that extend through modifying, transferring, and accepting specific risks, helping executives and boards understand the most likely paybacks on investments in security has been difficult. When possible, investments stretch from product and service purchases through employee training to insurance—the need for understanding the potential impact of an expenditure is great.

That brings companies to another approach—hiring an experienced consulting firm to conduct some or all of the risk quantification, framework building, and option development, with the goal of presenting the output to the executive board. While this approach will generally result in a briefing package for the board, it is expensive and tends to be transactional: the customer pays a fee and receives a desired product. This approach often does less than the "build it yourself" approach to increase staff expertise and raise the level of an organization’s cybersecurity maturity. The financial and organizational investments in this approach are frequently ongoing for extended periods of time.

Product/service overview

CDW's SPARQ is, at its core, a set of professional services supported by software; together, they act as a set of tools to help organizations understand their levels of risk exposure quantified in USD and choose the best options for responding to that risk. The information built on quantified risk, infrastructure inventories, security control, business priorities, and other data drawn from across the enterprise is analyzed as part of SPARQ and presented in various forms that can help executives and boards understand the strategies and investments for how best to modify, transfer, or accept the risk.

The overall goal is to present information that allows decision-makers to understand the best options that will allow the enterprise to modify risk so that it falls within the organization's appetite for, and tolerance of, risk. SPARQ is not, however, an advisory service for recommending specific products or purchases as might be expected of a service from a company that is among the largest resellers of information technology to enterprise customers. SPARQ is not a service offered by CDW's sales engineering group but a service of CDW's professional services organization.

SPARQ can be thought of as having three broad functions:

1. SPARQ quantifies risk

Because SPARQ is a professional service offering, it makes use of a third-party application for tasks such as risk quantification. CDW prefers to work with X-Analytics for the risk quantification portion of SPARQ due to factors including ease of reporting and its association with the National Association of Corporate Directors. X-Analytics is an eponymous SaaS-based tool that assesses risk for an organization and its individual business departments and operations then expresses that risk in USD.

X-Analytics provides the data on which significant portions of SPARQ's analytics components are based. While X-Analytics does not release an exhaustive list of its data sources, the company does say it draws on threat data, control effectiveness, loss probability, loss magnitude, and industry-based assumptions as it builds its quantification information.

X-Analytics is able to natively score cybersecurity maturity using any of five frameworks: CIS CSC Profile, CIS CSC Sub-Controls Profile, NIST CSF Profile, Foundational Controls Profile, and Technology Controls Profile. In addition, customers may request that X-Analytics data be applied to up to 19 additional cybersecurity frameworks for data sharing, scoring, and analytics.

2. SPARQ guides the prioritization of risks and risk responses

The CDW professionals and consultants delivering SPARQ use data from X-Analytics and other data-gathering tools and processes to build statements of prioritized risks and possible responses to those risks. These priorities are shown in dashboard form that helps executives and boards understand the priorities in both risks and responses and how acting on the responses will have an impact on the level of risk and the business.

SPARQ's delivery team builds on the data basis provided by risk quantification to help the customer understand a number of critical factors about risk, from the customer's appetite and tolerance for risk to the impact that risk could have on business plans to the most cost-effective possibilities for modifying the risk to fall within the customer's risk appetite.

There is a priority on information presentation and story in SPARQ because of the emphasis on moving the conversation on cyber-risk out of the cybersecurity group and into the business executive level. SPARQ includes dashboards and other presentation formats that are used consistently across different customers. As part of the service, CDW works with individuals to help them understand and share the story around quantified organizational cyber-risk.

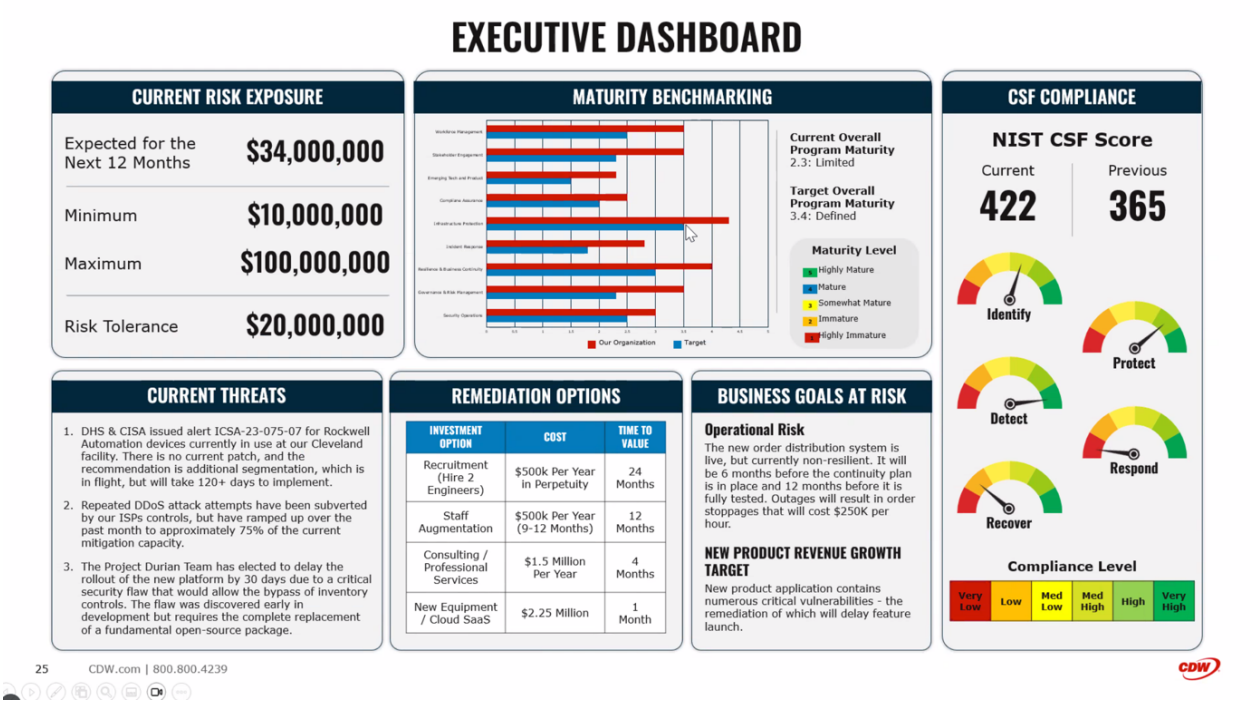
3. SPARQ helps customers tell their cyber-risk story to business executives

SPARQ is built on the understanding that there is limited usefulness in quantifying risk for its own sake. Taking the quantified risk from X-Analytics and using it to create a story to help make decisions about risk is one major step in the SPARQ service. Effectively telling that story to decision-makers at various levels of the organization is another major step.

For each of these steps, SPARQ provides not only output-containing information, but also scripting and coaching for the individuals who will be making the presentations. The delivery of the SPARQ service recognizes that there are different audiences of decision-makers, and that different audiences need different information presented in different ways. That basic recognition, and the element of communication and risk management coaching that happens as part of SPARQ, means that SPARQ is active in raising the customers' risk maturity level as it delivers information to the business as part of the service.

By having different service pieces that make up the SPARQ whole, CDW has made it at least theoretically possible for customers to engage CDW for part of SPARQ. In practice, though, CDW says that it is very rare for customers to take this piecemeal approach to the service. Generally, customers who purchase SPARQ want all the available options.

Figure 1: An example of the information and presentation typical of a dashboard for communicating the output of SPARQ to business executives



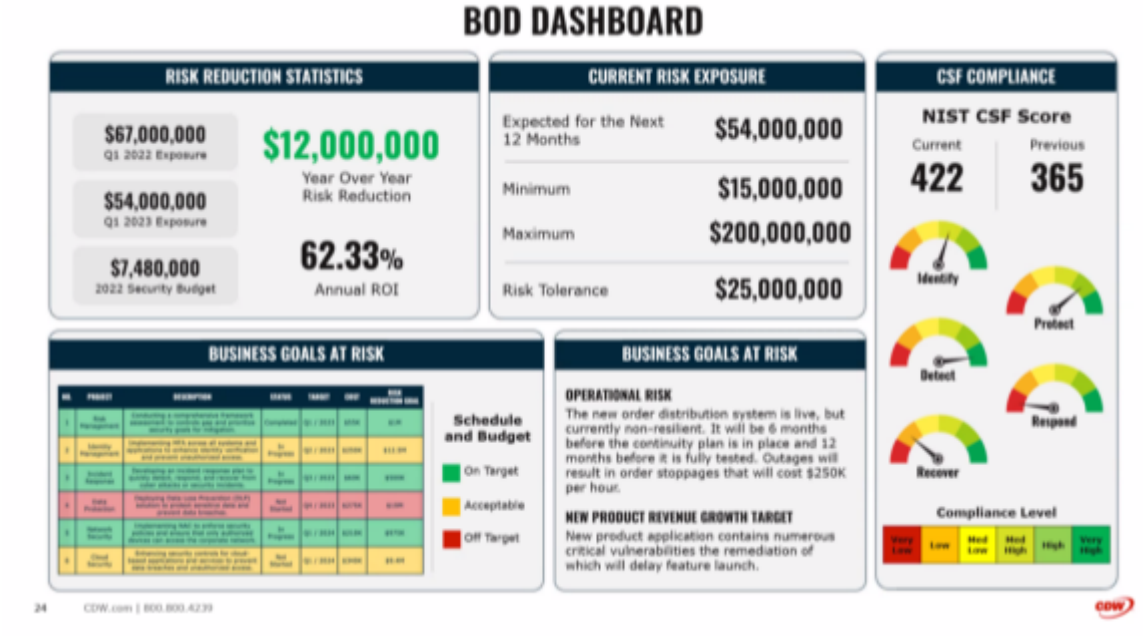
Source: CDW

CDW can configure output presentations to match a wide variety of requirements, from regulatory compliance audits to briefing books prepared for regular meetings of the executive board. Presentation materials and dashboards can be updated at regular intervals to aid the understanding of risk as a dynamic quantity rather than a static property of business that changes rarely, if at all. The typical SPARQ customer contracts for long-term (multi-year) assistance with an understanding of how various risks could impact the business, and what should be prioritized, and coaching to help managers better tell the story of risk-and-response to executives, the board, or other critical audiences.

It is at the end of this process, which includes quantification, context, and understanding investment, that SPARQ provides its greatest value. The real point of quantification, after all, is being able to do something about the organization's risk—to be able to modify or transfer risk so the overall level is within the organization's risk appetite. When the executive board can understand risk from a strategic level, and executives can see the most likely impact of tactical investments, all levels of the business can be involved at appropriate decision-making levels.

With regulators and law enforcement agencies requiring a more rigorous approach to risk management and the market closely following those requirements, the need for services such as SPARQ is set to expand as organizations continue to raise their security maturity levels.

Figure 2: An example of the information and presentation typical of a dashboard for communicating the output of SPARQ to an executive board



Source: CDW

According to CDW, while increasing a customer's security maturity level is part of SPARQ's goal, the maturity level does not start at zero—SPARQ is not a service intended to provide security expertise for a company that has none. It is also not intended for very small companies that need to contract with a security company in lieu of hiring one of their own.

SPARQ targets medium-to-large enterprise customers with a cybersecurity department but wants to increase security maturity and improve organizational security decision-making.

Because SPARQ is tailored for each customer according to the size and make-up of the organization, the complexity of their IT and cybersecurity infrastructures, and the degree of cybersecurity staff coaching required, amongst other factors, CDW says it is impossible to provide a "typical" contract cost for SPARQ. The company does say that they feel SPARQ is considerably less expensive than risk quantification and consulting contracts from competitors such as the Big Four (Deloitte Touche Tohmatsu (Deloitte), KPMG International (KPMG), PricewaterhouseCoopers (PwC), and Ernst & Young (EY)) consulting firms.

CDW sees the primary competition for SPARQ as service providers such as the Big Four consulting companies and major system integrators/consultants, along with failed internal projects to quantify risk according to one of the existing industry frameworks. The failed projects never lead to customers who simply want risk quantification, though: The risk quantification service within the overall SPARQ service is always performed as part of risk and mediation prioritization, followed by a communications playbook for one or more key internal audiences.

Company information

Background

CDW was founded in 1984 and began offering services in addition to products in 1987. The company completed an IPO and was listed on NASDAQ in 1993. CDW debuted on the Fortune 500 in 2001 (ranked

No. 23 as of 2023), was taken private in 2007, and re-listed on NASDAQ in 2013. It is a component of the S&P 500 index.

Current position

Headquartered in Vernon Hills, IL, CDW had revenue of $21.8bn in 2023. It has approximately 15,000 employees and more than 250,000 customers in more than 150 countries.

CDW offers SPARQ as one of its Amplified Security Services, which include offerings ranging from log aggregation and correlation to a Virtual CISO providing advice and coaching to a customer's CISO and security executives. CDW's professional services provide independent vulnerability assessments and advisory services to help customers identify gaps in security as defined by a range of cybersecurity frameworks and standards. The services cover actions ranging from tactical tasks such as deploying, monitoring, and managing security solutions to strategic services such as assuring security strategy alignment across the organization and communicating security strategy to the business organization.

CDW's position as a technology retailer gives it the possibility of partnerships with many different technology providers. The technology available to the company makes it possible to use solutions that work within a customer's own technology roadmap for many engagements and to bring “best of breed" technologies to play for many more.

Future plans

CDW's plans for SPARQ center on taking the service to additional customers in the existing customer profile. Beyond that, though, the customer profile could be expanded to include companies at earlier stages in their corporate growth or security maturity level.

In addition, CDW could consider bundling additional consulting and coaching services with SPARQ to make it a service that extends beyond risk quantification and prioritization to other facets of security and IT operations, such as pen testing for initial baseline measurement, breach planning capabilities, or virtual executives available on a fractional FTE basis. Any of these additional offerings would be presented as complementary to SPARQ rather than competing against any of its capabilities—SPARQ would remain at the core of this type of offering.

Key facts

Table 1: Data sheet: CDW

Product/service name	Security Program Assessment and Risk Quantification (SPARQ)	**Product classification**	Professional service
Version number	V1	**Release date**	Sept 2023
Industries covered	Multiple	**Geographies covered**	North America and Europe
Relevant company sizes	Mid-to-large enterprise	**Licensing options**	Custom contract
URL	cdw.com/sparq	**Routes to market**	Direct
Company headquarters	Vernon Hills, IL	**Number of employees**	15,000

Source: Omdia

Analyst comment

SPARQ is a fully formed service offering from a Fortune 500 company. It comes to the market with a well-defined target customer and sufficient supporting resources to meet those customers' needs. The questions regarding SPARQ revolve around whether it is a needed service and whether CDW is the ideal company to meet those needs.

The answer to the first question is a decided “yes.” The push to quantify risk and use that quantification to involve the executive board in security decision-making is firm and continuing. By focusing on executive coaching and communication with the business, CDW has put SPARQ in the middle of critical needs among all but the most security-mature organizations.

The answer to the second question is also “yes” given CDW’s long history as a technology provider and established reputation in the IT market. Though this kind of offering may challenge existing perceptions about what CDW can do, CDW's size has allowed it to hire experts in the field to act as consultants and advisors, combining individual expertise with CDW resources and experience to meet customer needs.

Those customers are well-defined and, in that definition, offer an opportunity to CDW's competitors. CDW is being specific about the companies it considers prospects for SPARQ, with mid- to large-size enterprises with established security programs at the heart of its target list. Thousands of smaller companies could reasonably look for security help from this source and, while CDW's reluctance to take them on makes business sense—in that smaller companies have a much different effort-to-return ratio—it does mean that those unserved companies are possible customers for other service providers.

Given the direction of the overall cybersecurity industry, it is

difficult to see a scenario in which SPARQ doesn't flourish. Potential competitors could do far worse than look at what CDW is doing with SPARQ and take notes. SPARQ is a solid offering that provides significant

strength at the very point where too many security offerings stop: the human communications and decision support that stretch out of the security group into the rest of the business.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

2024 Trends to Watch: Enterprise Security Management (December 2023)

Omdia Market Landscape: The Products and Players Driving the Fast-Growing Market for Cyber Insurance (October 2023)

Cybersecurity Decision Maker Survey 2023: Overall Findings & Enterprise Security Management (September 2023)

Author

Curtis Franklin, Principal Analyst, Enterprise Security Management

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com