CIO FROM IDG

SPONSORED CONTENT

Security Performance Management: Making the Most of Your Security Investments

Quantifiable measurements help organizations improve the effectiveness of cybersecurity programs and offer accountability.

Cybersecurity is consistently in the organizational crosshairs. Executives and board members want to be sure the enterprise is doing its best to avoid compromises and attacks.

Yet, how can executives be sure their security investments are making a difference? How can they identify gaps in security performance, while making decisions to better manage the effectiveness of their tools, technologies, and people?

Security Performance Management (SPM) helps companies answer these questions and more.

THE NEED TO CONTINUOUSLY MEASURE, MONITOR, AND MANAGE

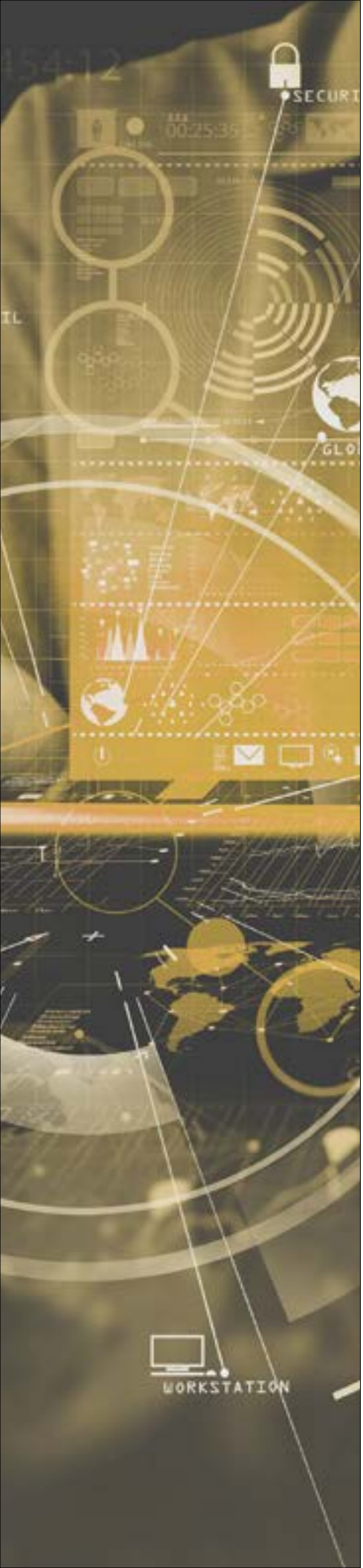
The stakes are high. Cybersecurity incidents can cause significant financial harm—including legal and cleanup costs, and increased insurance premiums—as well as serious damage to brand reputation, and the loss or theft of intellectual property and customer data.

It's because of these risks that security management takes up most of the CIO's time these days, according to the 2019 State of the CIO. Organizations are being held accountable for their security practices, outcomes, and failures by boards, executives, business partners, regulators, investors, and customers.

Successful security management requires performance measurement. It means having commonly accepted, objective, easily understood data—just like any other business function, such as finance (profit and revenue); HR (turnover and retention); marketing (lead generation, pipeline metrics, and conversion rates); and sales (new business and upsell data).

Cyber risk management up until now has taken a more traditional route. Organizations have been using methods such as audits, penetration testing, security assessments, and threat intelligence reporting to determine risk levels.

These approaches offer point-in-time operational metrics, not a continuous view of how security programs overall are performing. These results must often be translated or summarized for board meetings, where members might not understand, for example, if three security



incidents in one year is good, bad, or normal. Instead, leaders are left to wonder if their peers and industry competitors are faring better or worse with regard to security performance.

That's why organizations require a standard, objective, independent, and quantitative metric to assess and manage the ongoing performance of their cybersecurity efforts within the context of their industry and peer group.

Enter Security Performance Management.

GAINING INSIGHTS, FACTS, ANALYSIS

Security Performance Management (SPM) is a continuous, risk-based, outcome-driven approach to measuring, monitoring, and managing cybersecurity program performance. It drives accountability for security outcomes throughout the organization, while also ensuring that investments are actually efficient and effective.

There are five elements in a successful SPM strategy:

- **Key Performance Indicators (KPIs)**. Quantitative metrics are standardized, commonly accepted, and widely adopted. For example, security ratings provide a baseline measurement of cybersecurity performance that can help security and risk leaders make informed decisions quickly and effectively.
- **Planning and Forecasting**. There is regular goal setting and progress tracking because SPM facilitates data-driven, risk-based cybersecurity conversations among key stakeholders, including the security team, executives, board members, regulators, investors, and key business partners.
- **Allocation and Prioritization**. The use of objective data and peer group comparison helps identify gaps so that companies can allocate and prioritize efforts and resources.
- **Measurable Outcomes**. An SPM program measures outcomes. Doing so gives visibility into how cybersecurity programs are performing, enabling the business to align and adjust investments for impact over time.
- **Continuous Assessment/Monitoring**. SPM is focused on continual process improvements. By having access to security performance KPIs, the business can continuously and efficiently assess its security posture, reset program goals where necessary, track progress, and report meaningful information to executives and the board.

Combined, these elements reflect a mature cybersecurity program. An SPM strategy brings greater visibility, with context, into security performance. For example, by adopting security ratings, a company can see and compare their program's effectiveness to that of their peers and third-party organizations. SPM offers an intelligent, objective, data-driven method that allows the enterprise to shift from a reactive to proactive state.

SECURITY RATINGS FOR ACTIONABLE INFORMATION

Bill Brown, CISO at learning company Houghton Mifflin Harcourt (HMH), understands the need for a continuous security performance management approach. "At my previous company, I spent a lot of time helping the board of directors understand what they should

get from their security program. They always wanted to know how our approach to risk and security compared with our peers."

So, just over four years ago, he started using BitSight solutions, which help companies better manage third- and fourth-party risk, underwrite cyber insurance policies, benchmark security performance, and assess aggregate risk with objective, verifiable and actionable Security Ratings.

Similar to a credit score, the security ratings technology takes into account a range of indicators, including historical and security performance over time. The software-as-a-service platform gathers and stores billions of online events, and from this data it identifies:

- Infected machines
- Indications of compromise
- Proper or improper configuration of certain security controls
- Positive or poor security hygiene
- Potentially harmful user behaviors

This information is then applied to the company's network footprint, and analyzed for severity, frequency, duration, and confidence. Alerts are generated if a significant change occurs, and actionable insights are provided to mitigate risks. The ratings are updated daily, making it easy to manage and access for continual monitoring.

A CONTINUOUS MEASUREMENT OF PERFORMANCE

This data and visibility from BitSight offers great value to HMH. Brown says his company not only wanted to be able to compare its security program to peers, but also evaluate the risks around third parties like suppliers and vendors.

"Because the data is independent and objective, it gives us a good comparison," he says. "We also use the data to identify any gaps that appear externally so we can make improvements."

Brown cites this as a critical benefit. "We had an internal view of our security controls and program, but BitSight also offers us the external perspective of our security performance. It has given us a laundry list of improvements we could make; some we chose to do immediately, others over time. The tool helped our security team to prioritize those goals and objectives."

HMH uses BitSight to conduct weekly monitoring of its infrastructure, as well as assessments of third parties. "We get a rating, which I'm happy to report is on the upper average. We can see if there are any changes to our infrastructure that would affect the rating—either positively or negatively—and then we can evaluate and make sure we're closing any security gaps. Just doing periodic monitoring of our rating helps us maintain our security program."

Brown says that the Security Rating doesn't change drastically from week to week; over time, it provides considerably more visibility than HMH had before.

"Security performance management tools have raised awareness with regard to infrastructure and application changes," he adds, "helping us make sure we maintain our high standards—especially in terms of what's externally visible."

That awareness has made its way to the board of directors. "They're very interested in it,"

BITSIGHT: THE SPM LEADER

BitSight provides data-driven, independent and objective security metrics that help security and risk leaders to:

ASSESS PERFORMANCE OF CURRENT SECURITY POSTURE

ALLOCATE LIMITED RESOURCES AND PRIORITIZE SECURITY EFFORTS AND INITIATIVES

SET ACHIEVABLE SECURITY TEAM GOALS, AND TRACK AND REPORT ON PROGRESS OVER TIME.

BitSight for Security Performance Management (SPM) enables organizations to measure, monitor, and manage their performance similar to that of other key performance metrics.

BITSIGHT

Brown reports. "They want to know why our security performance is where it is, or why a competitor might be slightly above or below us in terms of security rating. Best of all, it gives them added confidence that we are focused properly on our security program."

MANUFACTURER DRIVES FACT-BASED CHANGES

In addition to raising awareness and improving confidence in the organization's security performance, BitSight helps measure the impact of security investments.

Take for example, STERIS, which develops and delivers a wide range of infection prevention equipment, products, and services. It's a growing company, with 12,000 employees and thousands of customers in 100+ countries.

With this growth have come new risks and challenges. STERIS wanted to assure customers that security is a priority, and clearly communicate its security status with employees and the board.

STERIS opted to deploy BitSight Security Ratings. The company is now able to measure risk levels throughout the organization, including all of its acquisitions. Any significant change results in an alert with details of malicious activity and forensic information, so the security team can quickly remediate.

In addition, the solution provides summary data and graphics with STERIS' security posture, enabling CISO Ed Pollock to make it clear to executive management and the board "that security investments are paying off."

SUMMARY

In today's high-stakes security risk environment, it's critical to understand how security investments are performing. Security performance management helps companies achieve that understanding, as well as identify gaps and set realistic goals.

Pollock says SPM insights have led to productive conversations with his peers. "I'm not just going to IT counterparts in our acquired companies and telling them what our best practices are and what they should do; I'm giving them data on the health of their security programs and having fact-based discussions about how to improve."

LEARN MORE ABOUT THE IMPORTANCE OF MEASURING SECURITY PERFORMANCE AND HOW TO GET STARTED AT BITSIGHT.COM.