Business Software Alliance

Cyber Vital Signs

How Better Metrics Can Improve How Boards and Executives Manage Cyber Risk

Organizations face rising cyber risks, and their boards and executives need better metrics to manage those risk effectively. Today's best measurements, like mean time to detect (MTTD) and mean time to respond (MTTR), are examples of data that boards and executives can leverage to manage cyber risk. However, these measurements are not universally used and more can be done to develop additional simple, fast, accurate, and complimentary metrics, designed to help boards and executives understand and manage cyber risks. These metrics, or Cyber Vital Signs, will enable organizations to more effectively manage cyber risk, and ultimately better serve customers and citizens, as well as build a more secure and resilient digital ecosystem. It is important that industry, government, and academic experts work to formalize a set of Cyber Vital Signs to help boards and executives measure and manage cyber risks.

Mean time to detect (MTTD)
The average amount of time from when a cyber event began to when it is detected.

Mean time to respond (MTTR)
The average amount of time from when a cyber event was detected to when it was responded to and mitigated.

The Growing Cyber Challenge

Around the world, digital transformation increases connectivity, improves customer and citizen experiences, and requires organizations to manage cyber risks and confront cyber threats perpetrated by malicious actors. These actors are increasingly sponsored or proteced by nation states that are increasingly fueled and protected by artificial intelligence (AI). In this new reality, the value of understanding the geopolitical landscape, including public policy and commercial diplomacy, and managing the risks associated with these changes is increasing.

Cybersecurity risk has bled from the war room to the boardroom. These challenges will only continue to increase in importance.

Today's Best Measurements

The cybersecurity community has improved cyber risk management, including by using measurements. For example, organizations have improved security by using secure software development best practices like those in the BSA Framework for Secure Software; developing better risk management frameworks and processes such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework; and enhancing training and educating a (still too small) cyber workforce. Leading cybersecurity companies are also leveraging AI for numerous security activities including threat detections and prevention, autonomous security operations, and predictive cloud security.

Additionally, boards and executives often leverage measurements like MTTD and MTTR to make data-driven decisions about cybersecurity investments. But because there are no formally recognized Cyber Vital Signs, not all organizations use these measurements, and the cybersecurity community has not fully explored identifying or developing complimentary metrics that would specifically help boards and executives manage cyber risk and quantifiably understand if organizations' cyber investments are fulfilling their promises.

The Stakes Are High

Incidents, increasingly perpetrated by malicious actors sponsored or protected by nation states, impose numerous costs on organizations and their customers. Those costs include:

- the theft of personal data and intellectual property
- the disruption of operations
- the damage to reputation and brand value
- the increase in insurance costs
- the rise in legal and regulatory compliance
- the pure financial loss associated with recovering from an incident
- the erosion of trust in the technology marketplace

Cyber Vital Signs

Peter Drucker wrote "What gets measured, gets managed." Today, boards and executives can use measurements like MTTD and MTTR to make data-driven decisions about cybersecurity investments. But by developing consensus Cyber Vital Signs we can both increase the use of these measurements and develop complimentary metrics designed specifically for boards and executives to fully understand the health and utility of their cybersecurity investments.

Metrology: The Driver of Progress

Metrology, the science of measurement, may seem like a dry and technical subject, but it is truly a vital and dynamic field that affects every aspect of human activity. Metrology provides the foundation for reliable and accurate information and innovation in disciplines ranging from trade and commerce to health and safety, from art and music to sports and entertainment.

Metrology helps establish tangible ways to measure abstract concepts, such as quality, performance, risk, trust, and security. These concepts are often hard to define and quantify, but they are essential for making decisions, solving problems, and achieving goals.

Without metrology, we would not have standard weights and measures, time zones and calendars, maps and GPS, thermometers, barometers, telescopes, microscopes, or many of the other countless devices that we use to observe, understand, and manipulate the world around us.

Metrology helps establish tangible ways to measure abstract concepts, such as quality, performance, risk, trust, and security. These concepts are often hard to define and quantify, but they are essential for making decisions, solving problems, and achieving goals.

Advances in metrology help to establish criteria, methods, and protocols for evaluating and comparing concepts, as well as ensuring that these measurements are consistent, valid, and reliable. Metrology also helps us to identify uncertainty, correct errors, and improve and refine our measurement systems and processes.

In sum, metrology was and remains the foundation for essentially every technological advancement that has improved our lives. It is time to bring the power of metrology to cyber risk.

Measuring Cyber Risk

Measuring an organization's cyber risk is challenging due to its inherently complex nature. The digital ecosystem consists of a vast array of diverse, interconnected, and dynamic people and technologies. Malicious actors range from state-sponsored advanced persistent threats to opportunistic cybercriminals to "script kiddies" whose impact can still be disproportionate to their knowledge or skill. Technologies range from physical hardware to applications, with countless providers competing and collaborating in those layers and the layers between.

Unlike fields with well-established metrological practices, cybersecurity has been slow to implement consensus measurements such as MTTD and MTTR, leading to inconsistencies in how organizations measure, report, and manage their security. This lag makes it difficult to gauge effectiveness or progress, as well as to compare cybersecurity across different organizations.

Cyber Vital Signs in Theory

Medical professionals begin to assess a patient's health using vital signs, such as body temperature, pulse, and respiration rate. These basic measurements do not provide all the information a medical professional might need, but they provide a fast and accurate foundation for collecting more detailed information and determining a treatment plan. They also provide a way to assess if a patient is improving as well as compare a patient with the broader population, each of which informs what interventions may be necessary.

Boards and executives have not yet adopted a comprehensive set of simple, fast, and accurate measurements, that is, we do not yet have Cyber Vital Signs.

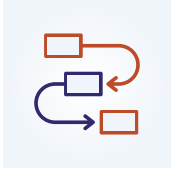
Just as vital signs do not provide all the information a medical professional may need or want to have before acting, Cyber Vital Signs may only provide a snapshot. But that snapshot can help boards and executives identify when they need to take immediate action, whether existing services are effective, and where to deploy more or different resources.

Cyber Vital Signs in Practice

Boards and executives might feel overwhelmed by the tools available to them today, many of which were not developed with them in mind. Organizations that select poor measurements, or no measurements at all, will spend limited resources to undertake suboptimal or ineffective activities while simultaneously feeling a false sense of security.

Cyber Vital Signs can help boards and executives understand and manage cyber risk, while also incentivizing their organization's business partners to find new and innovative ways to achieve better performance against them.

Leading businesses use cybersecurity measurements such as MTTD and MTTR to diagnose the health of their systems and these can be the foundation of a broader consensus on Cyber Vital Signs. Based on feedback from boards and executives about what metrics would be most valuable, cybersecurity experts can identify or develop complimentary metrics, which can translate the effectiveness of cyber investments, activities, and specific security controls and to reduced business risk.



Next Steps

Experience tells us that, with effort, we can improve measurements over time. That effort should be aimed at developing, testing, and validating metrics built for boards and executives. Good measurements exist and can be strengthened through recognition as Cyber Vital Signs and complimented with additional metrics. Experts from industry, government, and academia should begin building consensus around Cyber Vital Signs designed explicitly to help boards and executives manage cyber risks, as soon as possible.

TAKEAWAYS

- Boards and executives need a standardized set of Cyber Vital Signs to improve cyber risk management.
- Experts from industry, government, and academia can use metrology—the science of measurement— to build off existing metrics and formalize a set of core Cyber Vital Signs.
- By starting today and creating Cyber Vital Signs, experts in industry, government, and academia can deliver the metrics boards and executives need to improve cyber risk management.