What you don't know can hurt you

A big tech guide to risk measurement.

Big tech firms have put in some eye-catching growth numbers over the past decade. The so-called 'FAANG' stocks (Facebook, Amazon, Apple, Netflix and Google) have vastly outperformed other shares on the world's biggest exchange markets. Even Meta, the poorest performer of the illustrious group, has outgrown the S&P 500 by some 70%.

But success often breeds unwanted attention. In this instance, it manifests in more regulation and oversight by the federal government and regulators seeking to 'follow the money' (and be seen doing so). But governance, risk and compliance (GRC) isn't just a growing domestic concern – internationally, it's a similar picture with more scrutiny over privacy, liability and marketplace competition.

Coupled with this, the global economic downturn has shifted shareholders' and investors' attitudes to all forms of shares and stocks. Revenue growth is becoming less of a priority, with profitability reaffirming its position as the primary indicator of performance.

As a result of these two key trends, risk management has turned from a boardroom concern to an operational necessity. Enterprise CIOs, CEOs and CFOs are increasingly realizing that if they zero in on risk, they have a much better chance of protecting the zeros on the bottom line.

In this article, framed around the idea of "what gets measured, gets managed," we demonstrate how effective risk measurement can help put a dent in your risk exposure. We begin by exploring the four major difficulties that technology leaders face when seeking to quantify and report on risk across the organization.

Managing risks begins with measuring risks

But how do you measure risks in a meaningful way? Should you tally every software vulnerability in the company and its subsidiaries? Do you need to make a list of all the endpoint devices requiring software patches? Should you report the uptime stats for your company's most critical applications?

DIFFICULTY #1

Disparate, varied IT assets

Today, the IT estate needs to be cataloged and analyzed over, for example, 50 offices, 500 data centers (most of which belong to other companies), and 10,000 home networks. And a significant portion — probably at least 20% — of that distributed architecture consists of "shadow IT" — that is, products and services employees have adopted without formal approval and continuous oversight of the IT department. In this highly distributed, difficult-to-catalog IT environment, traditional risk-measurement tools and approaches simply won't work.

DIFFICULTY #2

IT complexity

It's not just that there are more devices; how software is built and works has changed. The age of large, monolithic applications is over. Today's IT infrastructure comprises lots of small and medium-sized components working together to create a greater whole. For example, an e-commerce application might rely on 75 different IT components to work. Those components might range from UI code to multiple back-end databases. The risks associated with each of those components affect the risks of the application overall.

DIFFICULTY #3

Sophisticated security attacks

Businesses are under attack by a growing collection of cybercriminals, many of whom have access to highly sophisticated technologies. In the beginning, cyber threat actors were mostly mischief-makers and computer programmers interested in finding ingenious ways to cause trouble. Today, attackers include nation-states, criminal syndicates, and malicious "script kiddies" willing to spend 50 bucks on the Dark Web to buy malware or a credential-stuffing script and a list of corrupted credentials.

DIFFICULTY #4

Shared responsibilities

A recent trend in risk management calls for sharing risks more broadly with business units. The IT organization might lead an organization's risk assessment project. But now, executive teams and boards of directors ask business-unit leaders to step up and take responsibility for the risks affecting their operations. To address these difficulties, take a top-down approach to measuring risk. Identify "supply chains" supporting each strategic goal and collect as much real-time information about the status of each supply chain as necessary.

Framing risk with strategic objectives

It's the job of the executive team and the board of directors to lead the company to achieve core objectives about business continuity, data privacy, and regulatory compliance. If you want to get the attention of your fellow executives, frame your discussion of risk measurements in terms of the board-level objectives. In other words, identify and weigh your company's various technical, regulatory, and other risks, and show how they relate to your company's high-level, strategic goals. You'll find that framing your risk measurements this way helps focus your work and improve the level of understanding and decision-making among line-of-business leaders.

Building a weighted scale for risks

It's rare for a company to treat all its strategic goals equally, but once you've identified those goals, assign them scores on some kind of scale, such as 1 to 10. For example, based on conversations with the executive team, you might assign continued revenue growth of at least 10% CAGR a score of 10, and regulatory compliance a score of 7.

Next, identify people, processes, and technology involved in supporting each strategic objective, and rank the importance of each of those supporting factors. To provide further nuance, you might estimate the likelihood of a particular type of failure occurring. For example, imagine your company has a web server supporting a business-critical mobile app. The odds of that server delivering unacceptably slow performance during a period of peak usage are probably higher than the odds of that same server succumbing to a power outage that crashes both the main and backup power systems.

By multiplying a score for the strategic importance of the server (say, 7 out of 10) by the likelihood of a specific risk (say, 50% or 0.5), you can begin ranking risks and identifying risks that require more immediate action.

For example, the server delivering slow performance might have a likelihood of 40%, and the server crashing in a catastrophic power outage might have a likelihood of 2%. If the server's importance is 7 out of 10, then the risk score for the slow performance scenario would be 7 times .40 (which yields 2.8). The risk score for the power outage scenario would be 7 times 0.02 (which yields 0.14). The slow-performance scenario, which has the higher risk score, is obviously the risk that needs attention first.

Bringing risk assessment into the age of cloud computing and WFH

Measuring risk used to be a special event undertaken with consultants. With real-time data and automation, companies now measure risk more accurately, continuously, and effectively. The first thing to change about risk assessments is their timeliness. Executives want to know if the risk mitigation measures that have been put in place are working. Risk teams should track the metrics that indicate whether or not the company is achieving its goals for managing risk.

Fortunately, IT departments have new tools that can help improve the speed and accuracy of risk assessments. Real-time endpoint monitoring, for example, can report on the location, IT health, and activity of endpoints at any location, including in home offices. This monitoring works over standard internet connections without requiring VPNs.

The other thing to have are data-driven conversations with the wider executive team about risk. Here's where that more timely and comprehensive data pays off. With improved visibility into endpoints and other IT assets, you can have a more meaningful discussion about which investments work and which don't. In addition, by taking advantage of real-time data and automation, companies can reduce risks and improve the security of their remote workforces at the same time.

Measuring risk is an ongoing strategic activity

You'll know if you have an effective practice in place for measuring risk if it provides ongoing guidance for making business decisions. To provide that guidance, your best practice for measuring risk should be continuously updated with information about your IT environment's current state. When risk data is current, you can trust that you're basing decisions on the technology and vendors you work with now, not a different set you worked with three months ago.