Why a holistic approach to managing risk is key to solving complex IT problems

Cybersecurity and reliability risks cannot be managed by working in silos. The key to solving complex IT operations problems collaboratively is to build a common engineering approach.

Jason Bloomberg
President, Intellyx

Cybersecurity threats and their resulting breaches are top of mind for CIOs today. Managing such risks, however, is just one aspect of the entire IT risk management landscape that CIOs must address.

Equally important is reliability risk – the risks inherent in IT's essential fragility. Issues might occur at anytime, anywhere across the complex hybrid IT landscape, potentially slowing or bringing down services.

Addressing such cybersecurity and reliability risks in separate silos is a recipe for failure. Collaboration across the respective responsible teams is essential for effective risk management.

Such collaboration is both an organizational and a technological challenge – and the organizational aspects depend upon the right technology.

The key to solving complex IT ops problems collaboratively, in fact, is to build a common engineering approach to managing risk across the concerns of the security and operations (ops) teams – in other words, a holistic approach to managing risk.

Risk management starting point: site reliability engineering

By *engineering,* we mean a formal, quantitative approach to measuring and managing operational risks that can lead to reliability issues. The starting point for such an approach is *site reliability engineering* (SRE).

SRE is a modern technique for managing the risks inherent in running complex, dynamic software deployments – risks like downtime, slowdowns, and the like that might have root causes anywhere, including the network, the software infrastructure, or deployed applications.

The practice of SRE requires dealing with ongoing tradeoffs. The ops team must be able to make fact-based judgments about whether to increase a service's reliability (and hence, its cost), or lower its reliability and cost to increase the speed of development of the applications providing the service.

Error budgets: the key to site reliability engineering

Instead of targeting perfection – technology that never fails – the real question is just how far short of perfect reliability should an organization aim for. We call this quantity the error budget.

The error budget represents the total number of errors a particular service can accumulate over time before users become dissatisfied with the service.

Most importantly, the error budget should never equal zero. The operator's goal should never be to entirely eliminate reliability issues, because such an approach would both be too costly and take too long – thus impacting the ability for the organization to deploy software quickly and run dynamic software at scale.

Instead, the operator should maintain an optimal balance among cost, speed, and reliability. Error budgets quantify this balance.

Bringing SRE to cybersecurity

In order to bring the SRE approach to mitigating reliability risks to the cybersecurity team, it's essential for the team to calculate risk scores for every observed event that might be relevant to the cybersecurity engineer.

Risk scoring is an essential aspect of cybersecurity risk management. "Risk management… involves identifying all the IT resources and processes involved in creating and managing department records, identifying all the risks associated with these resources and processes, identifying the likelihood of each risk, and then applying people, processes, and technology to address those risks," according to Jennifer Pittman-Leeper, Customer Engagement Manager for Tanium.

Risk scoring combined with cybersecurity-centric observability gives the cybersecurity engineer the raw data they need to make informed threat mitigation decisions, just as reliability-centric observability provides the SRE with the data they need to mitigate reliability issues.

Introducing the threat budget

Once we have a quantifiable, real-time measure of threats, then we can create an analogue to SRE for cybersecurity engineers.

We can posit the notion of a threat budget which would represent the total number of unmitigated threats a particular service can accumulate over time before a corresponding compromise adversely impacts the users of the service.

The essential insight here is that threat budgets should never be zero, since eliminating threats entirely would be too expensive and would slow the software effort down, just as error budgets of zero would. "Even the most comprehensive… cybersecurity program can't afford to protect

every IT asset and IT process to the greatest extent possible," Pittman-Leeper continued. "IT investments will have to be prioritized."

Some threat budget greater than zero, therefore, would reflect the optimal compromise among cost, time, and the risk of compromise.

We might call this approach to threat budgets *Service Threat Engineering,* analogous to Site Reliability Engineering.

What Service Threat Engineering really means is that based upon risk scoring, cybersecurity engineers now have a quantifiable approach to achieving optimal threat mitigation that takes into account all of the relevant parameters, instead of relying upon personal expertise, tribal knowledge, and irrational expectations for cybersecurity effectiveness.

Holistic engineering for better collaboration

Even though risk scoring uses the word *risk,* I've used the word threat to differentiate Service Threat Engineering from SRE. After all, SRE is also about quantifying and managing risks – except with SRE, the risks are reliability-related rather than threat-related.

As a result, Service Threat Engineering is more than analogous to SRE. Rather, they are both approaches to managing two different, but related kinds of risks.

Cybersecurity compromises can certainly lead to reliability issues (ransomware and denial of service being two familiar examples). But there is more to this story.

Ops and security teams have always had a strained relationship, as they work on the same systems while having different priorities. Bringing threat management to the same level as SRE, however, may very well help these two teams align over similar approaches to managing risk.

Service Threat Engineering, therefore, targets the organizational challenges that continue to plague IT organizations – a strategic benefit that many organizations should welcome.

Learn how Tanium is bringing together teams, tools, and workflows with a Converged Endpoint Management platform.

Tanium, the industry's only provider of converged endpoint management (XEM), leads the paradigm shift in legacy approaches to managing complex security and technology environments. Only Tanium protects every team, endpoint, and workflow from cyber threats by integrating IT, Compliance, Security, and Risk into a single platform that delivers comprehensive visibility across devices, a unified set of controls, and a common taxonomy for a single shared purpose: to protect critical information and infrastructure at scale.

Visit us at www.tanium.com and follow us on LinkedIn and Twitter.

Intellyx is the first and only industry analysis, advisory, and training firm focused on customer-driven, technology-empowered digital transformation for the enterprise. Covering every angle of enterprise IT from mainframes to artificial intelligence, our broad focus across technologies allows business executives and IT professionals to connect the dots on disruptive trends.

Read and learn more at intellyx.com or follow them on Twitter.