ICIT Institute for Critical Infrastructure Technology

The Cybersecurity Think Tank

Malcolm Harkins

ICIT Fellow & Chief Security and Trust Officer, Epiphany Systems

Avoid Sisyphus - Progressing Beyond the Motion(s) of Cybersecurity

AN ICIT FELLOW PERSPECTIVE
JULY 2022

Introduction

In Greek mythology, Sisyphus was the founder and King of Ephyra (now known as Corinth). Zeus punished him for cheating death twice – forcing him to roll an immense boulder up a hill only for it to roll down whenever it approached the summit, repeating this action for eternity. Sisyphus was burdened by an exhausting, perpetual, uphill struggle in which he could never achieve sustainable progress or momentum. He was locked in a doomed routine that drained his attention, effort, and resources. Through the classical influence on modern culture, tasks that are both laborious and futile are described as Sisyphean. In many organizations, cybersecurity leaders are self-punishing by relegating their efforts to trite solutions and tired methodologies that are too inefficient, ineffective, and inexpedient to deter modern adversarial campaigns, let alone adapt to or preempt sophisticated attack paradigms. In short, by not adopting a progressive strategy that aligns with the organization's strategic mission, capabilities, and priorities, cybersecurity leaders are preordaining a Sisyphean task. Their resources are squandered, and the ultimate culmination of their effort is to be crushed by the burden of the task and reset at square one.

A Newtonian Spin on Cybersecurity

The field of cybersecurity, or Information Security at a higher level, benefits from interdisciplinary approaches to provide novel strategies and perspectives, especially when the lessons borrowed from other disciplines are fundamental, foundational, universal, and accessible to a broad audience. In physics, the laws of motion denote how speed, velocity, and acceleration govern our natural world. At the macroscopic, we process progress and action through the operations of motion; meanwhile, at the molecular level, matter and the reactions that create our world are all due to nanoscale particles' speed, velocity, and acceleration.

The physics of motion is well documented, and we understand how these scalar and vector quantities differ. In information security and cyber risk management, the dynamics of change are not as well understood, which has confounded/muddled our ability to distinguish between motion and progress. This confusion has created a Sisyphean condition that intensifies our escalating risk cycle by causing a mirage of control that continues to lead us down a path of compromise and catastrophe, adding not only to our growing cyber labor shortage but also generating implications for societal risk on a grander scale.

Let's start with some basics on the physics of motion. Speed is a scalar quantity which is a measurement of magnitude regardless of direction, such as 55 MPH. In the cyber context, a measure of motion would be things like patching hygiene levels, time to detect, time to contain, or a wide variety of other vulnerability management and attack surface measurements traditionally used in our security operations as well as board reporting on how well we are doing with respect to our cyber defenses. These are context-less measurements that offer data but not insight.

The problem with using these types of measurements in the cyber context is that we are confusing motion for progress. This focus on motion leads to more of the same broad-based spray and pray approach we have been perpetuating for decades. We create goals for ourselves to patch faster, monitor more, reduce time to detect, and reduce time to contain. While these have added some value, they have also increased our total cost of controls and, in some cases, created a false sense of security and an inaccurate portrait of the actual risk. We are doing more without consideration for why we are doing it or whether the operation has a meaningful impact or achieves the desired outcome(s). The result we have achieved is the creation of continuous laborious and seemingly futile tasks.

To achieve real progress in cybersecurity, we need to have measurements that are vector quantities like velocity or acceleration. Vector quantities are a better approximation of progress because they include the magnitude and a clearly articulated direction that the internal and external observers can objectively understand. A correlating example of this would be 55 MPH northeast. So, now we know where we are headed in addition to how fast we are getting there, and our direction and measurement are universally understood and free of ambiguity. In cybersecurity, mitigating risk is challenging and may be daunting; but it is by no means impossible. A proactive trajectory depends on moving toward a clear goal at a manageable pace in an unwavering direction to reduce risk and the total cost of controls. In the cyber context, this would be things like understanding the anatomy of an attack before a breach occurs so that points along the potential attack paths can be understood and actions can be taken to disrupt adversarial motion. This sort of attack path analysis is where we can demonstrate actual risk reduction because steps have been taken that reduce attacker opportunities, not just on an initial point of compromise but on the entire attack path that leads from that initial foothold through our organizations to the point of material impacts such as the loss of sensitive IP or PII, or a critical system taken offline.

In physics, the momentum of an object is determined by its mass and velocity. In cybersecurity, the momentum of your efforts depends on the pace you move to address an issue and the weight (i.e., resources and priority) you apply to mitigation and remediation efforts. With the proper prioritization on materially impacting conditions that create exposure, we can have more leverage to decrease the mass needed (less resource consumption) to gain cyber momentum.

Meanwhile, acceleration - the integral of velocity - is the overall measure of the change in velocity (speed and direction) over time. Your organization's cybersecurity acceleration is characteristic of how quickly you react to measurements, how efficiently you implement necessary organizational change, and how nimbly you adapt to changes in the threat landscape. Changes in direction and speed happen and are a natural factor of sustained progress, but your overall acceleration should be positive. It should not be understated that you may need to slow down or stop to reevaluate the best direction and pace to achieve positive change.

Finally, the force of your effort is the product of the acceleration and the weight you applied. In physics, force, acceleration, and velocity can all be measured as component vectors in their associated XYZ directions. In cybersecurity, to achieve a "force multiplier," you must develop efforts in multiple directions and ensure they are not conflicting.

Leveraging the ‘Physics of Cybersecurity’ to Define Attack Scenarios

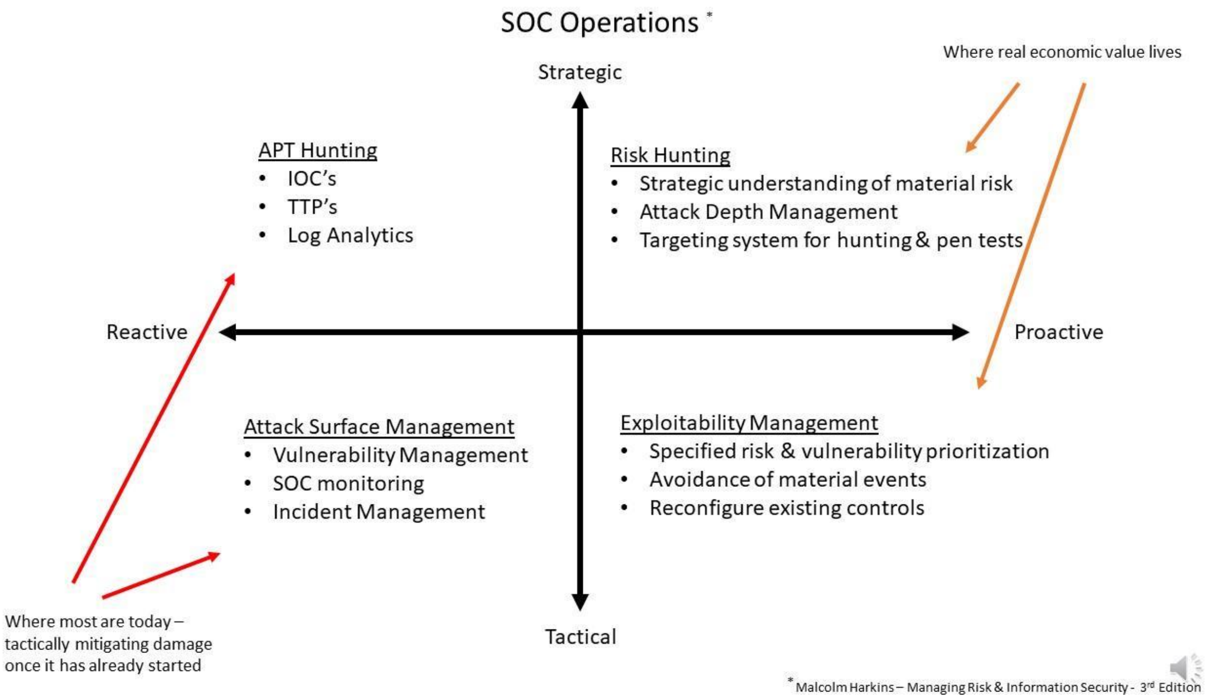
Understanding these attack paths with speed empowers teams to contextualize measurements, break attack paths, and prioritize detection and response controls along these attack paths. This would accelerate our proactive risk mitigation due to the specific direction (coordinates) provided. So, how do we reorient our entire security operations function so that it is optimized to handle the volume of activities for which it is responsible? How do we reposition ourselves from an anchor point of continual reaction to one where our SOC can take proactive action in front of the cycle of risk?

The heart of these changes is a redefinition of the risk equation we have been using for decades.

FROM: Risk = F (Threat, **Vulnerability**, Consequence)

TO: Exposure = F (Threat, **Exploitability**, Consequence)

But first, we need to realize that vulnerability does not equal exploitability. Secondly, we must recognize that exposure to a material impact should be an organization's primary focus. Last, we need the capability to easily map these attack paths and understand the exploitable pivot points that lead from the initial foothold or point of compromise through our environment to the catastrophe that causes exposure to material impact for our organizations and our customers. When both conditions are met, we can optimize our security operations by shifting from only an anchor point of reaction to proactive cyber risk management.


SOC Operations *
Where real economic value lives
Strategic
APT Hunting
• IOC's
• TTP's
• Log Analytics
Risk Hunting
• Strategic understanding of material risk
• Attack Depth Management
• Targeting system for hunting & pen tests
Reactive
Proactive
Attack Surface Management
• Vulnerability Management
• SOC monitoring
• Incident Management
Exploitability Management
• Specified risk & vulnerability prioritization
• Avoidance of material events
• Reconfigure existing controls
Where most are today – tactically mitigating damage once it has already started
Tactical

* Malcolm Harkins – Managing Risk & Information Security - 3rd Edition

Figure 1 depicts a security operations framework for proactive cyber risk management.

As shown in Figure 1, security operations can be framed according to a simple framework the author has created and strived to achieve over the years. We can categorize our work on the vertical axis from tactical to strategic. Being strategic means doing what is necessary to identify and achieve the organization's long-term interests. Our organizations strategically want a bend in the curve of risk they are experiencing as well as a reduction in the total cost of controls. Both of which have been growing for decades.

We can categorize our work on the horizontal axis from reactive to proactive. Proactive means creating or controlling a situation by causing something to happen rather than responding to it after it has happened. So being proactive by almost every implication would lower risks and costs, especially if you had the specific coordinates (devices, identities, applications, network segments) within your enterprise to break attack paths before an event occurred.

Refocusing Our Corporate Cybersecurity by Understanding the Variables

So why are most security operations anchored in tactical reaction with limited strategic reaction activities such as APT hunting? Many would argue it is due to resource constraints. They don't have the budget, don't have the talent, and don't have the tools. While this may be true in some cases, consider that we are in this situation because of the paradigm with which the entire security industry has been built.

In cybersecurity, the most frequently asked question focuses on "who" is behind a particular attack or intrusion – and may also delve into the "why." We want to know who the threat actor is, whether it is a nation-state, organized crime, insider, malicious individual, or some organization to which we can ascribe blame for what occurred, and the damage inflicted. Those less familiar with cyber-attacks may ask, "Why did they hack me?" As someone responsible for managing information risk and security in the enterprise for 20-plus years, I can assure you that we have no real influence over threat actors and agents - the "threat" part of the above equation.

These questions are rarely helpful, providing only psychological comfort, like a blanket for an anxious child, and quite often distract us from asking the one question that can make a difference: "HOW did this happen?" But even those who asked HOW answered with simple vulnerabilities – we had an unpatched system, lacked MFA, or the user clicked on a link.

The current focus on the WHO, WHY, and HOW based on vulnerability does minimal service to the industry and community. As mentioned earlier, we need to rethink and refocus the Security Risk Equation to examine the intricate details of how attacks really occur to prevent them in the future. We need to have a continuous offensive perspective for our defense controls.

The primary variable in the security risk equation that I have the maximum chance to impact risk is where my organization is exploitable. From a consequence and impact perspective, we need to focus only on three primary consequences: Confidentiality, Integrity, and Availability (CIA triad). Depending on the attacked technology or data, each of these has different potential impacts to an individual, an organization, or society. When we examine "how" attacks are accomplished, we see three core targets for attacks:

- Attacks on identity credentials
- Attacks focused on the execution of malware
- Attacks that create a Denial-of-Service (DoS)

So, what must always be analyzed, acted upon, and reported to management is HOW an intrusion or attack could be successful. Afterward, we can provide prescriptive recommendations on eliminating attack paths and where to prioritize detecting anomalous activity to intercept attackers before a material event occurs.

At Epiphany Systems, we set out to solve this problem which resulted in a transformative capability that predicts not only the initial point of compromise and how it will bypass your current endpoint controls detailing the entire attack path that any adversary would most likely use for an attack PRE-BREACH. Our recommendation engine tailors specific actions that can be taken to break any spot along the attack path before it occurs. In doing so, we illuminate the complete exploitability of your entire organization, not just the exploit of a simple vulnerability that an attacker would use for an initial foothold. Our goal is to enable security operations to take proactive steps tactically and strategically to lower your risks at a lower total cost.

Conclusion

T. Dewar, the famous Scottish distiller, once said, "Minds are like parachutes; they work best when open." I would invite you to open your minds and imagine a new paradigm for your security operations, a new approach to managing and measuring risk with exploitability as the fulcrum of this transformation.

About Epiphany Systems

With news stories of cyberattacks breaking daily, even the largest and best-staffed organizations cannot stay in front of issues that create risk. Environments are increasing in complexity, and attack surfaces are growing to a point where siloed and tool-centric solutions cannot adequately reduce risk. Preventing a material event is about visibility and prioritization – two things the cybersecurity industry has failed to provide effectively. Epiphany Systems solves these problems by taking a proactive perspective and providing decision intelligence. Our solution provides visibility, prioritization, and mitigation of risks by focusing on the material impact to resources critical to your organization and the quickest way to minimize your exposure. We leverage machine learning and patented technology that interacts with existing controls. Changing focus from threat hunting to continuous exposure management enables organizations to mitigate against potential damage before it ever happens.

About Malcolm Harkins

Malcolm is an ICIT Fellow and the Chief Security & Trust Officer with Epiphany Systems. He is also independent board member and advisor to several organizations. He is also an executive coach to CISOs and others in a wide variety of information risk roles. Malcolm engages in a wide variety of peer outreach activities to drive improvements across the world in the understanding of cyber risks and best practices to manage and mitigate those risks. Key areas of focus include the ethics around technology risk, social responsibility, total cost of controls, and driving more industry accountability. Previously Malcolm was the Chief Security and Trust Officer at Cylance was also previously Vice President and Chief Security and Privacy Officer (CSPO) at Intel Corporation.