Wilson Perumal & Company

WP&C VANTAGE POINT

CYBER OPERATIONAL CULTURE

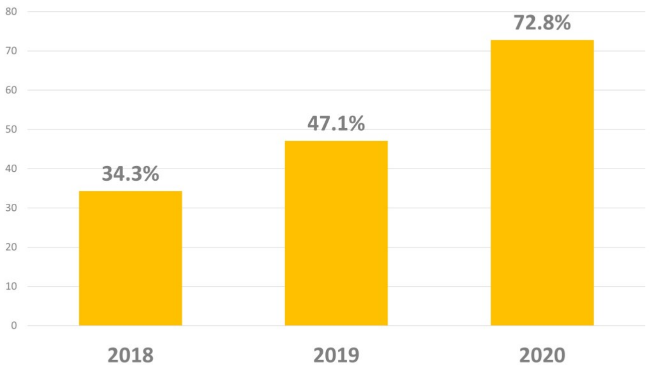
Human performance is the key to protecting organizations and saving the cyber insurance industry

Cyber Insurance Needs A New Strategy to Survive

Cyber insurance was a fledgling industry only ten years ago. Today, the global cyber insurance market is worth $7.4 billion and is expected to grow to $20.6 billion by 2025 to meet demand. But as cyber attacks increase, insurance companies are experiencing mounting losses resulting from their inability to quantify cyber risk and price coverage accordingly.

Cyber insurance payouts to clients are now increasing faster than premiums for coverage. Cyber insurers themselves, such as AXA, are also increasingly the targets of successful cyber attacks.

CYBER INSURANCE LOSS RATIO INCREASES



Source: Cybersecurity and Identity Theft Insurance Coverage Supplement; spglobal.com

In response to reduced profitability, many cyber insurers are blindly increasing premiums and deductibles, lowering coverage, and imposing new strict rules for customers. Some insurers may be forced to stop underwriting cyber risk entirely.

For the cyber insurance industry to survive, it must find new ways to accurately model cyber risk.

Predictably, new technology-focused upstart cyber insurers are emerging—attempting to disrupt the traditional cyber insurance industry by developing technology offerings which they hope will reduce customers' cyber risk and increase visibility into customers' risk.

But even this new breed of cyber insurer will ultimately fail because the risk-reduction assistance they are attempting to deliver to customers is insufficient and focused in the wrong area.

WP&C's analysis confirms that 85%–95% of cyber incidents and breaches are the result of well-understood, preventable failures in human performance that stem from poor operational discipline.

Operational Discipline Improves and Leverages Human Performance Rather than Replacing it

Poor human performance is the root cause of most cyber risk.

Increasingly frequent catastrophic cyber attacks threaten global health care, banking, transportation, and energy infrastructure and terrorize businesses of all sizes. The true source of cyber risk remains largely misunderstood and misdiagnosed, causing cyber insurers to incorrectly analyze and underwrite risk.

When IT operations lack effective mechanisms to detect failures in operational discipline and build a high-reliability culture, companies easily succumb to cyber attacks, despite being compliant in their adherence to cybersecurity frameworks and standards.

Existing cybersecurity risk assessments have proven to be woefully insufficient and unreliable. Insurers are essentially flying blind—often relying on simple customer questionnaires to assess complex cybersecurity controls (like Zero Trust Architecture) and lacking any verifiable data on the performance of the people responsible for those controls.

As a result, **insurers cannot accurately analyze and underwrite risk, exposing them to large payouts to clients and an unprofitable business model.** In fact, a focus on audits tends to encourage a “checkbox mentality” that undermines developing a culture of cybersecurity vigilance and accountability.

The unfortunate truth is that there is a fundamental problem with the traditional compliance-oriented approach to cybersecurity that pervades organizations that depend on frameworks alone.

A new approach is desperately needed—a high reliability approach focused on improving human performance rather simply attempting to replace the human element with more technology and automation.

This idea is recognized in the International Journal of Human-Computer Studies: “Treating everyone as a problem does not seem to work, given the current cyber security landscape.”

Benefiting from research in other fields, we propose a new mindset—’Cybersecurity, Differently.’ This approach rests on the fact that the problem is actually the high complexity, interconnectedness, and emergent qualities of socio-technical systems. Well-intentioned humans can be important contributors to organizational cybersecurity, as well as be “part of the solution” rather than “the problem.”[1]

We define operational discipline as doing **the right thing, the right way, every time**

[1] Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

WP &C Wilson Perumal & Company

High Reliability Organizations offer a blueprint for how to improve Operational Cyber Discipline

In our cybersecurity article published in MIT Technology Review, we argue that to reduce cyber risk, companies should look to High Reliability Organizations (HROs) to learn how to instill practices and principles that transform underperforming organizations into high-performing organizations that demonstrate consistent cyber operational discipline.

An HRO is an organization that experiences fewer anticipated events of harm while operating in complex, high-risk environments.

HRO principles have been successfully used for decades to safeguard NASA, the Nuclear Navy, the FAA, Johns Hopkins, PG&E, and the Mayo Clinic, to name a few. The principles and practices that make HROs so successful in other domains are focused on improving human performance and building a culture of operational discipline and excellence.

They are rooted in well-established behavioral science that has proven its value over more than sixty years of academic study. These principles and practices are readily transferable to the cybersecurity arena. But IT has not been the focus for organizations adopting HRO practices—that must change if cyber risk is to be meaningfully reduced.

The International Journal of Human-Computer Studies continues, “Socio-technical systems are complex, highly interactive and unpredictable, and adverse events have multiple contributing factors. Moreover, contrary to being the primary source of all problems, humans can be a vital player in defending against attacks (Hatekar et al., 2018). Labelling human actors as “the problem” does not acknowledge their ability to detect anomalies and halt attacks.[2]

As losses mount for cyber insurers and premiums soar for their enterprise customers, both groups now recognize the current risk management strategy has failed. Insurers must become a catalyst for change—encouraging customers to prioritize elevating human performance and building a cyber-resilient culture.

Doing so requires:

1. Carefully assessing how process complexity and culture contribute to behaviors that increase cybersecurity risk
2. Working with customers to reduce adverse IT and business process complexity that contributes to human error
3. Working to adopt the HRO practices and principles that provide safeguard against individual failures in human performance while developing a cyber-resilient culture
4. Developing the leadership and tools to institutionalize learnings and to sustain gains in human performance and culture, despite of changes in personnel
5. Routine reassessment of culture, complexity, and operational discipline

[2] Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem” to a ‘human-as-solution” cybersecurity mindset. International Journal of Human-Computer Studies, 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

THE PATH FORWARD FOR INSURERS:

Collaborate with customers to increase operational discipline

Cyber insurers should adopt an approach similar to that of the health insurance industry. Customers can take a physical to set a baseline premium, and health insurers then provide discounts, as customers work to improve their health through gym memberships and other healthy lifestyle practices. The end result is a win-win: health insurer risk is reduced and customer health is improved while premiums stay flat.

Similarly, in the future, cyber insurers will incorporate complexity, culture, and operational discipline assessments to more accurately assess baseline risk and set premiums. They will then provide incentives for discounts focused on making meaningful improvements in these areas.

For cyber insurers to create sustainable profitability going forward, they must partner with customers to improve cybersecurity human performance and operational discipline through the adoption of complexity-reduction strategies and HRO practices and principles.

Organizations must:

- Baseline their current cyber culture, complexity, and operational discipline to reveal their sources of behavioral cyber risk
- Identify high-impact, quick-win opportunities and close those gaps before reassessing and choosing the next opportunities

Closing these gaps will require designing and executing culture alignment plans to improve areas of cyber operational discipline weakness, and also continually measuring organizations' cyber operational discipline to ensure continued risk mitigation, future improvement, and quick intervention when necessary.

The good news is that with the right tools and team, this transformation can start to rapidly produce results. The key to success is developing a plan that is fit-for-purpose for your organization and aligning all levels of leadership on the benefits of executing the plan. These include ancillary benefits that often go beyond reducing cyber risk and can result in unintentional but positive improvements in both resilience and risk reduction across many other complex areas of the organization's operations.

Recognizing human performance as the root cause of the vast majority of cyber incidents—and promoting effective culture and behavioral interventions to address this critical area—is essential for cyber insurers to stay in business and for organizations to reduce risk.

Are you interested in discussing operational discipline as a tool to understand and mitigate cyber risk?

START THE CONVERSATION >

Wilson Perumal & Company *offers unparalleled support to improve Operational Discipline and transform companies into High Reliability Organizations. We use our deep expertise in technology complexity to help organizations implement HRO principles to reduce incidents and compliance risk.*