Wilson Perumal & Company

WP&C VANTAGE POINT

WILL YOUR ENTERPRISE SURVIVE THE CYBERSECURITY WAR?

Transforming cyber-operational discipline is the only path to protection

A sobering dose of reality:
Companies are failing to address their biggest source of cyber risk

Enterprises are losing the cybersecurity war, and the worst is yet to come. Global cybercrime is predicted to inflict damages of $6 trillion USD annually this year[1] . However, next year, IT annual budget growth is projected to grow at only 6.5%[2] , with small annual increases in IT headcount—while cloud services spending is expected to top the chart of IT priorities.

By 2025, cybercrime is predicted to be larger on an annualized basis than the GDPs of Japan and Germany combined—$10.5 trillion USD—making it equivalent to the size of the world's third-largest economy, after the United States and China[3] .

The economic damage caused by the pandemic will pale in comparison to the damage expected to be inflicted by cyber-attacks to our health care, banking, transportation, and energy infrastructure. The scope and scale of the coming crisis transcends industries, politics, and borders. No organization is fully protected.

Unfortunately, the true source of cyber risk is often misunderstood and almost always goes unaddressed. Breaches are rarely the result of novel hacks that exploit 'zero-day' vulnerabilities. Instead, they are largely the result of common, well-understood, and easily avoidable failures in human performance. These failures are the hallmarks of poor cybersecurity operational discipline.

The growing threat of cyber attacks

Cyber threats are more frequent, harmful, and costly than ever before

MERCK

June 2017
The drug and vaccine maker suffered worldwide disruption of operations when it was the victim of an international cyberattack, halting drug production and costing the company $1.3B

solarwinds

March 2020
The major US information technology firm was the subject of a cyberattack that spread to its clients undetected for months, doing as much as $100B in damage

Colonial Pipeline
May 2021
The American oil pipeline system was a victim of a ransomware attack—the largest cyber attack on a US oil infrastructure target—halting operations and shutting down delivery of 45% of all oil used on the East Coast for several days

Operational excellence and discipline are largely missing from cyber security

IT organizations often talk about developing a 'culture of operational excellence', but few know how to actually do so. Legacy IT service management frameworks (like ITIL, COBIT, etc.), although widely adopted, have failed to bend the cyber risk curve down. Similarly, cybersecurity risk management frameworks (like NIST, ISO 2700x, SOC2, etc.) have also proven insufficient to the task. These frameworks fail because they are not effective in developing a culture that embraces operational excellence or ensuring operational discipline within an organization.

A major component of operational excellence involves building a culture that cares about operational discipline—people doing the right thing, at the right time, every time.

Failures in cybersecurity operational discipline have been identified as the overwhelming source of cyber risk.

A Ponemon Institute report found that 34% of organizations hit by data breaches in the previous two years knew their systems were vulnerable prior to attack[4]. Dark Reading Magazine reported that 60% of organizations that had reported a data breach in the previous two years cited a known, unpatched vulnerability as the culprit.[5]

The rapid movement of IT infrastructure to public clouds and the shift to remote work have further heightened cyber risk by increasing IT complexity. This requires a shift away from the traditional perimeter-security-based trust model to a "zero trust architecture." Hackers are increasingly able to find vulnerable IT resources within most enterprise public clouds or to compromise vulnerable home networks.

Finally, the IT and cybersecurity labor shortage is getting worse, exacerbated by a recent surge in companies hiring IT professionals due to increased cyber threats and overworked employees leaving the profession. Globally, there are currently 3.12 million unfilled cyber security positions, ranging from entry-level analysts to executive -level leaders.[6] These factors indicate that already poor cyber operational discipline is almost certain to further deteriorate and further increase cyber risk.

WHAT IS OPERATIONAL DISCIPLINE?

Knowing the right thing to do

Doing the right thing the right way

Ensuring others always do the right thing

Why is it so difficult for IT and cybersecurity organizations to achieve cyber operational excellence?

Most IT operations either lack sufficiently formalized safety checks, balances, and accountability processes or execute them poorly when they do have them. IT organizations often rely on informal processes to ensure the performance of critical tasks, and they rely on their execution by a small, trusted cadre of knowledgeable, skillful, and dependable professionals.

However, organizational performance is rarely dependable or consistent without a high-reliability culture and a systematic approach to creating and sustaining a high level of human performance. Key to a high reliability culture is establishing formalized processes and accountability, yet most IT organizations operate on a 'best-efforts' basis, ignoring these critical elements.

Common organizational failures from insufficient formality and accountability include missing critical cybersecurity patch notifications or failing to act on them.

Hackers only need a single unpatched, exposed system to gain access, move laterally, and wreak havoc. The rapid adoption of public cloud-based virtual machines and containers has significantly increased the risk that IT operations may miss patch notifications or lose track of vulnerable resources.

While many IT organizations sense that they lack operational excellence, most are holding out hope that some future technology will emerge to save them and reduce their dependence on fallible humans. Unfortunately, new technology still requires humans to administer and operate it successfully.

Simply adding more (and more complex) technologies, without first developing a foundation of cyber operational excellence increases cyber risk, instead of reducing it. Is there a better way? Are humans really "the problem" and, if so, what can we do about it?

FAILURES IN CYBERSECURITY OPERATIONAL DISCIPLINE ARE RESPONSIBLE FOR MOST CYBERBREACHES

60%

of reported breaches are attributed to vulnerabilities unpatched due to human error

22%

of reported breaches cite misconfigurations resulting from human failure

You cannot automate your way to cyber operational excellence

Global spending on information security and risk management services is forecast to jump to $150 billion this year.[7] Much of this spending is focused on increasingly automated technologies that promise to reduce cyber risk by removing dependence on the human element.

While emerging intelligent cybersecurity technologies—such as SD-WAN, cloud access service brokers, secure service edge, etc.—play an important role in reducing cyber risk and enabling the transition to a zero-trust architecture, these technologies can only be successful if accompanied by disciplined human performance of both enterprise IT teams and end-users of IT systems.

Improving employee cybersecurity awareness, behavior, and culture remain some of the most challenging obstacles to dramatically reducing cyber risk. No matter how much automated technology is used, employees continue to be vulnerable to socially engineered cyber-attacks.

In the area of IT processes, automating IT systems administration simply moves the human performance risk to whomever is responsible for maintaining the reliability and security of the automation.

In fact, over-reliance on automation tends to make humans less vigilant and less prepared when automation fails. Even the latest AI-based technologies have failed to improve the situation and, in fact, are likely to introduce new sources of cybersecurity vulnerability that IT professionals are woefully unprepared to address.

The truth is that most enterprise IT executives are flying blind—lacking any meaningful visibility or insight into their organizations' true cybersecurity effectiveness and lacking the tools to improve it.

While many large enterprises have hired Chief Information Security Officers (CISOs) and have made large investments in well-designed defensive cybersecurity architectures and adoption of cybersecurity standards, none of these steps (on their own or collectively) have been able to demonstrate meaningful reductions in human error and improvements in cyber operational excellence.

But enterprise IT departments are not the only type of organization to have faced the challenge of reducing risk by improving human performance and developing a culture and capabilities to deliver operational excellence.

Complex businesses successfully managing high-risk, high consequence of failure operations exist in many sectors, including nuclear energy, aviation, chemical manufacturing, and healthcare.

Elite, operationally excellent organizations in these sectors have mastered the ability to operate at high levels of operational discipline and have been doing so successfully for decades.

The same principles they use to managed operational risk are needed to achieve cyber operational excellence.

5 CYBERSECURITY OPERATIONAL EXCELLENCE REQUIREMENTS THAT ENTERPRISES STRUGGLE TO ADDRESS TODAY

Knowledge of what cybersecurity operational excellence looks like and what it takes to achieve it

Policies, processes, and controls up to operational excellence

IT employees properly executing processes and controls in a timely manner

A management system that allows professionals to quickly catch and correct errors

An environment that demands learning from mistakes and rapid improvement

The Solution: **Adopt the practices of High Reliability Organizations to achieve cyber operational excellence**

Successfully managing risk in complex and high consequence of failure environments is not rocket science. It has long been the domain of organizations dubbed High Reliability Organizations (HROs)—which are defined as organizations that experience significantly fewer accidents, incidents, or events of harm, despite operating in highly complex, high-risk environments.

The US Nuclear Navy is commonly accepted as the original HRO, having operated nuclear-powered warships under the most demanding of conditions successfully since 1955 without a single reactor accident.[8] Many other organizations, including world-renowned healthcare institutions such as Johns Hopkins Hospital and Health System, the Mayo Clinic, and the Cleveland Clinic, have adopted and successfully applied the principles and practices of High Reliability Organizations. Doing so has allowed these leading organizations to transform their quality of care and reduce risk in healthcare operations.

The secret to the success of HROs is a shift in perspective about the nature of the problem that stands in the way of achieving operational excellence. In non-HROs, human fallibility is viewed as the principal obstacle to be overcome.

These organization usually adopt a compliance-oriented approach—focusing on improving policies, processes, training, and awareness of the nature and sources of risk. There is nothing wrong with doing these things. But HROs recognize that complex socio-technical systems are, by their very nature, unpredictable and prone to failure in unanticipated ways. In such environments it is foolhardy to expect that humans will not fail.

Instead of seeing human failure as the problem to be solved, HROs focus on designing systems and processes that are resilient in the face of inevitable human failure.

Instead of expecting organizations to get things right, HROs focus on developing the capability to learn quickly from mistakes and to effectively propagate those learnings. Instead of focusing on trying to constrain human behavior (effectively turning people into machines) to achieve "compliance", HROs give people the flexibility to develop and use their judgment and recognize the enormous value of human judgment when placed in unpredictable circumstances. HROs never focus on individual blame (during root-cause analyses). Instead, they make it easy to admit individual failure, knowing that integrity and transparency are hallmarks of high-performing organizations.

Enterprise IT organizations must learn from HROs and adopt a new way of working—called Cyber HRO, based on the proven principles and practices of demonstrated high-reliability organizations—to enable IT teams and end-users of applications to achieve and sustain the highest level of human performance and operational discipline.

CYBER HRO DEFINITION

A Cyber HRO is defined as an organization that experiences significantly fewer adverse or harmful cybersecurity and cyber-resilience events than others operating in the similar environments, while preserving its operational effectiveness and efficiency.

To become a Cyber HRO and reduce cyber risk, IT organizations must adopt the 'HRO Five Pillars of Operational Discipline'[9]—designed to ensure that the organization—not just an individual—to do the right things, the right way, every time.

THE HRO 5 PILLARS OF OPERATIONAL DISCIPLINE

Formality

Level of Knowledge

Forceful Watch

Questioning Attitude

Integrity

Cyber HRO principles and practices will deliver true cyber operational excellence for the first time

HROs achieve their high levels of performance through practice, not quick fixes and Cyber HRO is no different in that regard. But, IT organizations that diligently adopt the 'HRO 5 pillars of Operational Discipline' will significantly reduce the errors in human performance that lead to most cybersecurity incidents and breaches.

If cyber HRO is the solution, why haven't IT organizations adopted HRO practices in the past?

One reason is that most IT organizations struggle under budget constraints and traditional HRO methodologies have historically appeared to be costly and labor intensive. Another reason is simply a lack of awareness and understanding of the benefits of HRO. But, the most significant reason IT organizations have not adopted HRO practices is that the enabling tools to support efficient cyber HRO transformations have not previously existed. To date, traditional HRO adoption has been supported by methodologies and training that is not easily accessible and have not been refined for the digital age.

Now, a new class of management system—called the Cybersecurity Operational Excellence Management System (C-OEMS™)—exists to bring the proven benefits of HRO to enterprise IT and cybersecurity organizations for the first time, and in a cost-effective manner.

HRO PRACTICES HAVE YIELDED DRASTIC REDUCTIONS IN HUMAN ERRORS IN HEALTHCARE

GENESIS

100%

decrease in incidents from 2009 to 2017

JOHNS HOPKINS

79%

decrease in incidents from 2017 to 2021

Cincinnati Children's

67%

decrease in incidents from 2005 to 2009

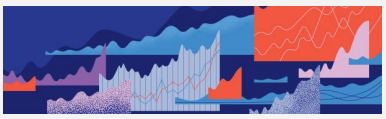
Introducing the Cybersecurity Operational Excellence Management System™

Effective management systems are a critical part of building operationally excellent organizations. Yet IT departments—and most importantly, cybersecurity professionals—have never had an operational excellence management system of their own.

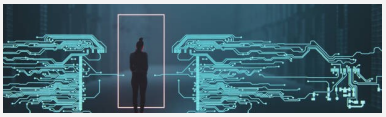
The C-OEMS™ provides a framework to integrate HRO principles and practices into modern IT and cyber security operations. This framework is designed to provide enterprises with supportive tools to monitor, analyze, control, and continuously improve operational discipline and human performance in a manner that enables true cyber operational excellence.

Regardless of future escalation by cyber threat actors, or the increasing complexity of supporting new technologies and architectures, enterprises that apply C-OEMS™ techniques to IT and cybersecurity domains will be enabled to dramatically improve human performance, reduce cyber risk, and improve business resilience.

THE C-OEMS™ FRAMEWORK PROVIDES ENTERPRISES WITH:



An ability to assess their level of cyber operational excellence and identify areas of risk



Effective HRO cyber culture interventions for both application end-users and IT/cyber administrators

Cyber HRO optimizations that deliver a high level of operational discipline for IT/cyber processes

Tools to rapidly improve and maintain the highest standard of cyber operational excellence

A cyber operational excellence governance model that is tailored to your organization

Why the Cybersecurity operational excellence management system works

- **Provides a Cyber Integrated Management System that brings together cyber/IT policies and standards with proven HRO practices and principles**
- **Formalizes and optimizes IT runbooks to ensure IT cybersecurity policies and processes are designed to HRO standards**
- **Provides cybersecurity operational excellence KPIs and anchors culture transformation in operational excellence objectives**
- **Uses a cyber operational excellence governance model to ensure KPIs are actionable at all levels of the organization**
- **Provides standards and methodologies for holding supply chain and services partners to a high level of cyber operational excellence**
- **Leverages your existing Governance, Risk, and Compliance (GRC) platform as a part of your integrated risk management capability**

When using a C-OEMS™, enterprises have the tools to greatly reduce their biggest source of cyber risk—poor human performance and lack of operational discipline.

These tools help to shift the organization's human resources from being viewed as a liability to being viewed as an essential asset in the battle to against cyber crime. By using a C-OEMS™ in conjunction with modern cybersecurity standards and a Governance, Risk and Compliance (GRC) system, enterprises can easily demonstrate the impact of Cyber HRO to customers, insurers, and regulators.

Regardless of the intensity of the future cyber threats, or the growing complexity of the IT landscape, a Cyber HRO, like all other types of HROs, will be best prepared to defy the odds, successfully manage the ever-changing risks, and operate in a safe and highly resilient manner.

AREAS OF APPLICATION FOR C-OEMS™ TECHNOLOGY

IT Operations

Cyber Operations

Employee Behavioral Discipline

Incident Response

Disaster Recovery

DevOps/ SRE

Software Supply Chain Security

ABOUT WILSON PERUMAL & COMPANY

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.

To learn more, please contact us:

contact@wilsonperumal.com

www.wilsonperumal.com

WP&C's Cybersecurity Perspective