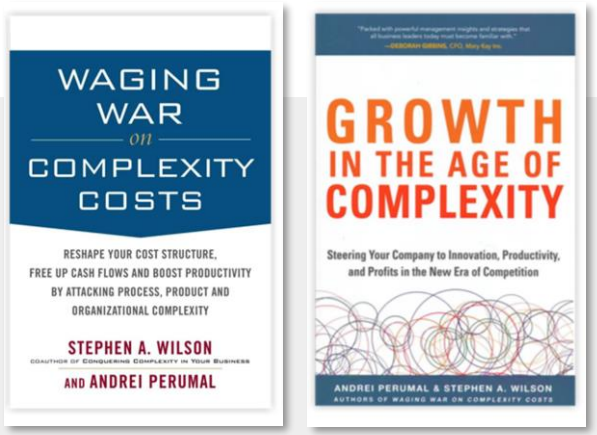
Wilson Perumal & Company
EXECUTIVE WEBINARS

People are Assets, Not Threats:

The Missing (but Essential) Piece of your Cybersecurity Strategy

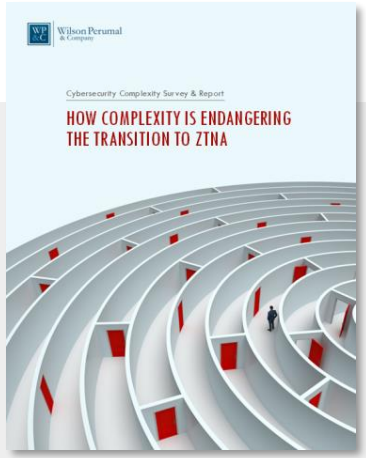
WATCH THE WEBINAR

There is a clear link between IT complexity and cybersecurity risk



We wrote the books on complexity

Human errors increase in complex environments



WP&C's first-of-it's-kind study to explore the effects of complexity on cybersecurity and ZTNA

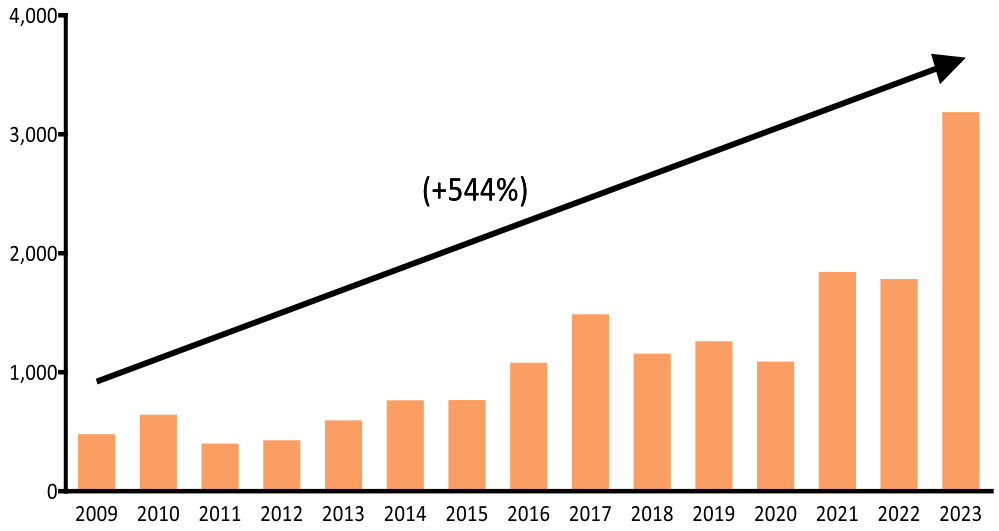
Complexity undermines cybersecurity effectiveness

We have unique insights into improving human performance in complex environments

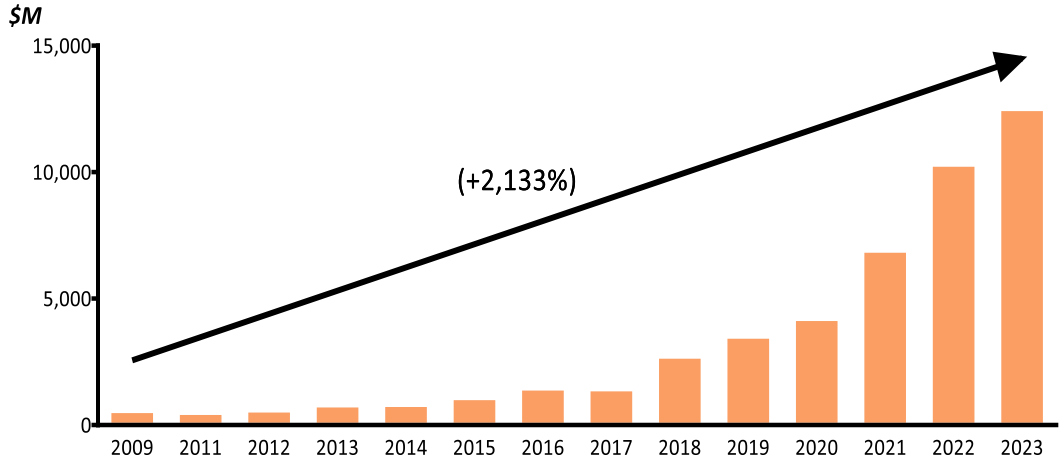
Your team members are essential to your cybersecurity strategy

Cyber attacks continues to rise and are getting exponentially more costly despite billions spent annually on cybersecurity technology

ANNUAL CYBER ATTACKS IN THE U.S.



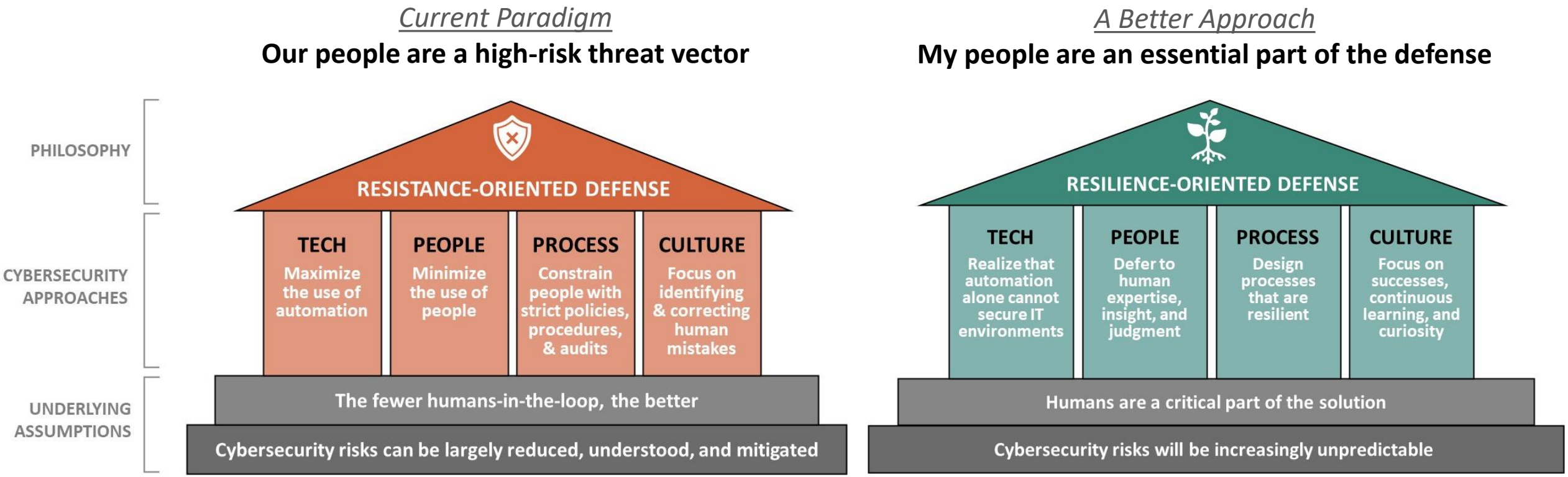
ANNUAL AMOUNT OF MONETARY DAMAGE CAUSED BY REPORTED CYBERCRIME IN THE U.S.



More than $220B was spent defending against cyber attacks in 2023, and spending is expected to be $500B by 2030!

Sources: Identity Theft Resource Center, FBI Internet Crime Report; Grand View Research

95% of cyber attacks are caused by human error, but traditional approaches try to solve the "people problem" the wrong way



High Reliability is a proven approach to quickly turn people in your organization into a highly effective and essential part of your defense strategy

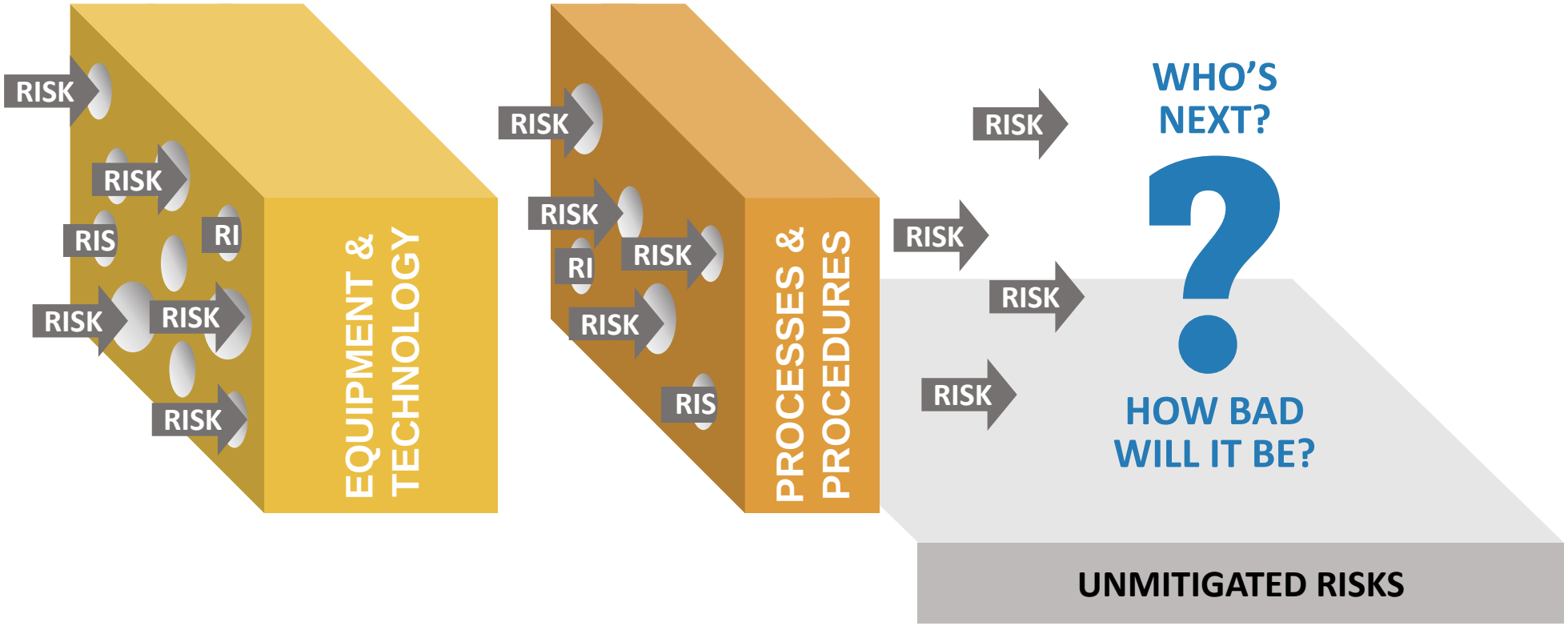
Cyber attacks are expected to cost victims $9.5 trillion in 2024!

RECENT INCIDENT	IMPACT	WHAT WE KNOW
UnitedHealth Change Healthcare: **Ransomware Attack**	• Patient care for 100M+ people disrupted • $850M+ impact; 94% of US hospitals affected	• Recycled passwords available on dark web provided access • Good password hygiene has been a "best practice" for 20+ years
Arup (British engineering group): **Deep Fake Impersonation of Corporate Executive**	• $25M transferred out of the company by employees to scammer accounts	• CFO was impersonated using AI generated voice and images • Multiple "confidential transactions" were directed by the fake CFO
Hewlett Packard Enterprise: **Multi-Factor Authentication Bypass**	• Company's MS Office 365 email system compromised • SharePoint was compromised—providing access to cybersecurity team data, cloud infrastructure, and other departments	• Multi-factor authentication was in use • Social engineering and password spraying used to defeat MFA

Although some attacks are getting more sophisticated, many people fail to do the basics: use strong passwords & don't recycle them, don't click unverified links

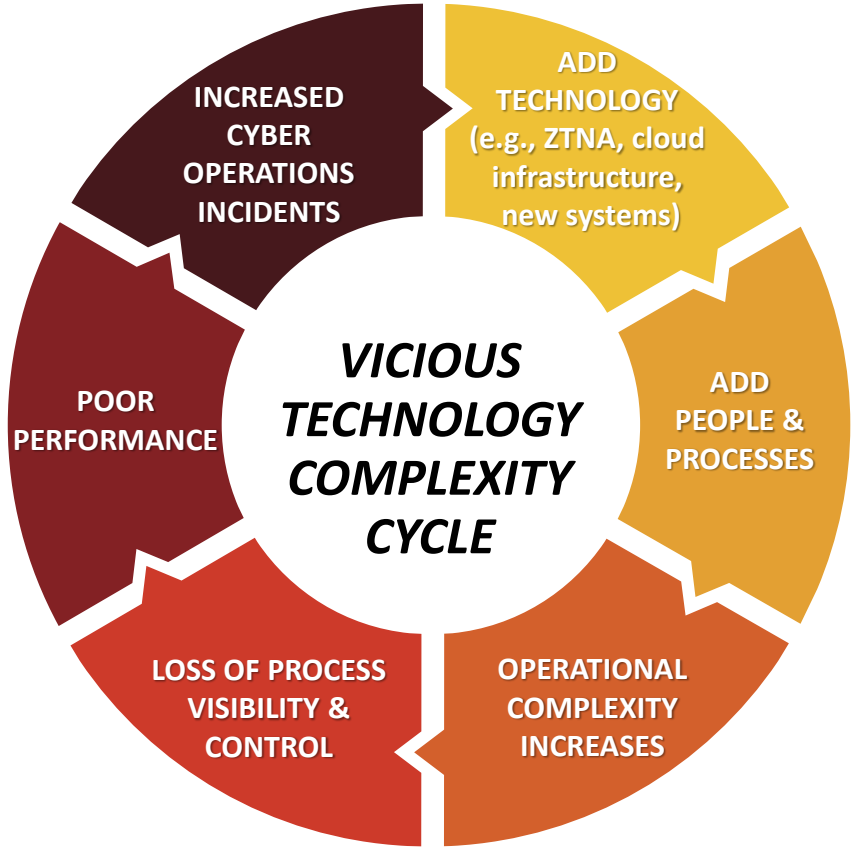
Sources: Cobalt IO; Ninjio

To create a secure cyber environment, we have focused on installing security equipment, technology, and the processes to operate them



These unmitigated risks raise many uncomfortable questions that leaders are hoping they don't have to answer first-hand

The technology-first approach to cybersecurity has created a vicious cycle that is adding risk and undermining our tech defenses



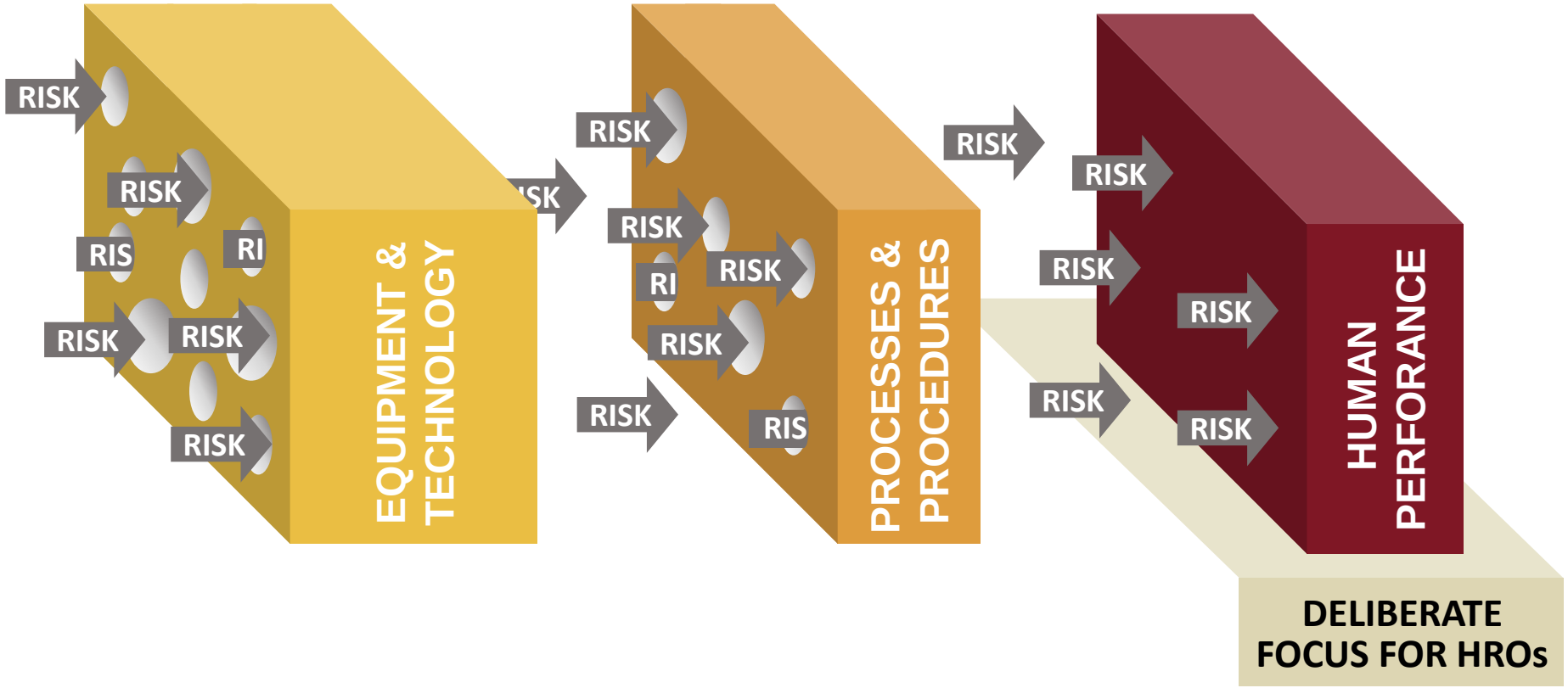
Technology-first is failing because:

- Our operating environment and systems have become so complex no one can fully understand them
- People will continue to make mistakes—further undermining efforts to control inputs, processes, and outcomes
- Resource demands (time, capabilities, dollars) have grown past most organizations' ability to supply them—85% of IT vulnerabilities remain un-remediated 30 days after announcement

Our approach to cybersecurity must change to become more effective

Source: 2024 Verizon Data Breach Investigations Report

The different approach needs to enable resilience and be adaptable to an ever-changing environment



High Reliability Organizations have successfully tackled the "95% problem"

High Reliability Organizations have remarkably low numbers of incidents despite performing highly-complex and hazardous tasks

5 Characteristics of HRO Mindfulness


Preoccupation with failure


Reluctance to simplify


Sensitivity to operations


Commitment to resilience


Deference to expertise

"HROs are distinctive because of their efforts to organize [and operate] in ways that increase the quality of attention across the organization, thereby enhancing people's alertness and awareness to details so that they can detect subtle ways in which contexts vary and call for contingent responding (i.e., collective mindfulness)."

HROs have created deep resilience to guard against the errors, mistakes, omissions, and breakdowns that can lead to catastrophic outcomes

Managing the Unexpected: Assuring High Performance in the Age of Complexity. Weick, K., Sutcliffe, K. (2001)

High Reliability Organization (HRO) evolution has enabled organizations to adapt and maximize the benefit of new technology

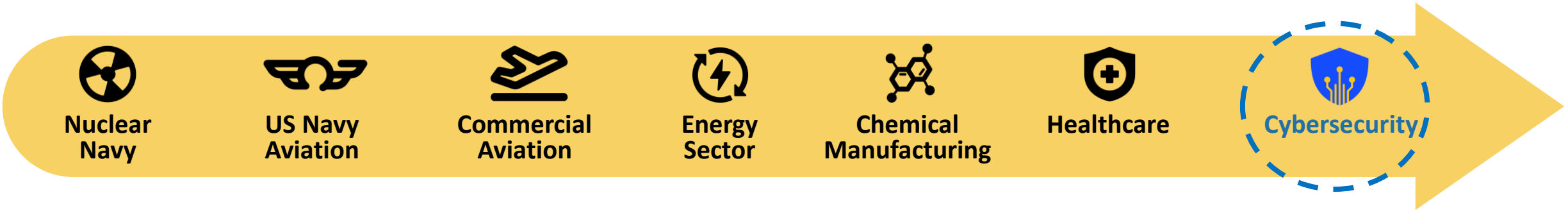
1950s
HRO principles evolved after World War II from the U.S. Navy's program to develop and deploy mobile nuclear reactors to power ships and submarines

1960s – 1970s
HRO principles then started to take hold across select, high-risk, and operationally-complex sectors

1980s – 1990s
Researchers at Berkeley and University of Michigan study the U.S. Navy, FAA, and a commercial power plants to understand how these organizations operate

1990s – 2010s
Most recently, HRO principles have been deployed in other environments such as chemical manufacturing and emergency care "High-Reliability Healthcare"

TODAY
IT HROs are a needed revolution in cybersecurity—High Reliability Cyber Orgs(HRCs) will maximize human capability to prevent catastrophic cybersecurity failures



Impact of HROs

No catastrophic nuclear incidents while operating ~150 mobile Navy nuclear reactors for 60+ years

33x reduction in commercial aviation fatalities per million miles flown since 1973

100% decrease in incidents at Genesis Health System from 2009 to 2017

HROs know they can't rely only on technology, procedures, and training to effectively mitigate risks in a dynamic environment

	TYPICAL APPROACH *Known risks are managed, only when everything goes to plan*	VS	THE HRO APPROACH *The system is designed to detect and respond to known and unknown risks*
 **EQUIPMENT & TECHNOLOGY**	Install well-engineered, constructed, tested, and maintained equipment and expect it will perform as designed		Assume that even the best equipment and technology at some point will break-down and fail
 **PROCESSES & PROCEDURES**	Develop rigorous procedures to eliminate employee guesswork		Assume even the best procedures will fail to anticipate all contingencies
 **HUMAN PERFORMANCE**	Hire and train capable employees that can correctly follow the established procedures		Implement well-developed practices to catch and react to breakdowns across all three tiers (including fellow employees)

HROs build resilience in dynamic operating systems by learning, sharing, and acting on information that others typically overlook (weak signals)

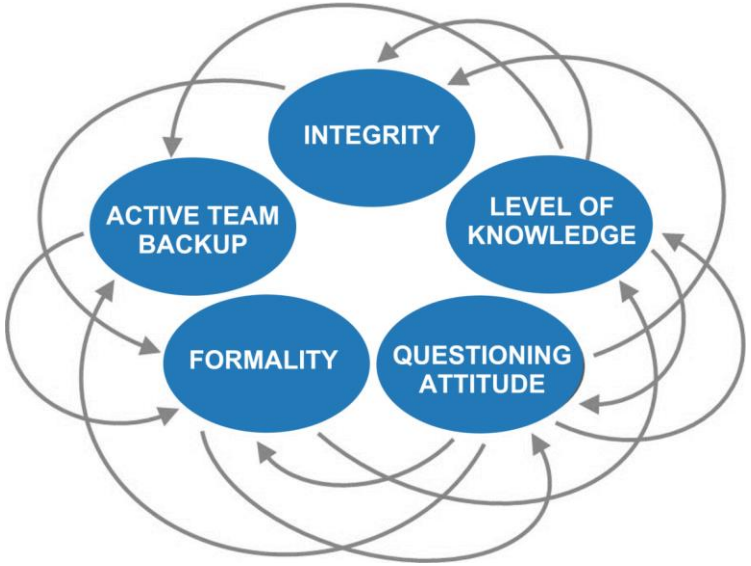
All high-performing organizations share a similar set of traits (HRO Pillars) that define operational values and guide behaviors

HRO PILLARS

The Pillars guide the behaviors and ways of working at every level and for every role in the organization

THE PILLARS WORK AS A SYSTEM

While each trait has both positive and negative expressions, the system of traits together enhances desirable actions and subdues potential negative behaviors

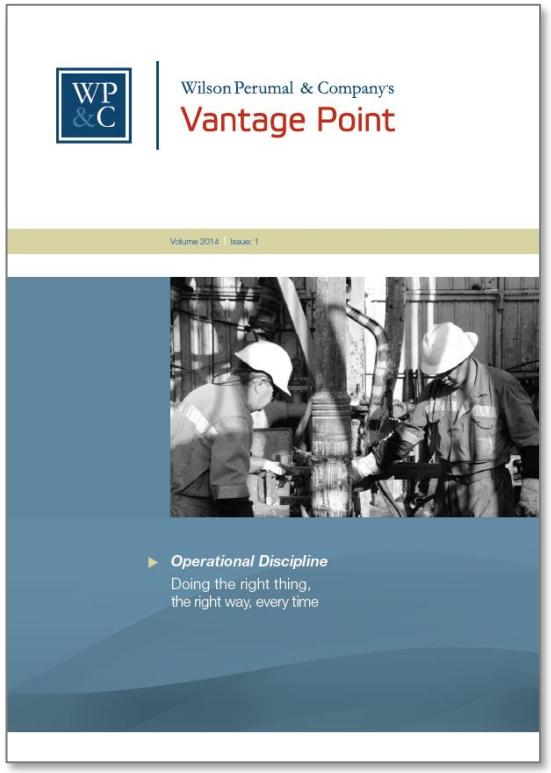


Human performance is the biggest lever to improve performance against the dynamic, quickly evolving, and weak signals that can result in high-consequence failures

Simply telling employees to adopt new values doesn't work—the new values must be tied to work practices

PILLARS	OPERATIONAL VALUES	OPERATIONAL PRACTICES
Formality	All employees exhibit a seriousness about what they do. They communicate in exact, prescribed terms. They understand & respect procedures.	• Procedures are followed explicitly; a formal process is used to update them • Risk analysis drives the use of verification checks • Post-mortems are done with structure; action items assigned and tracked
Level of Knowledge	All employees understand not only what they do but why. They continually seek greater knowledge, not just of their immediate work area, but also around it.	• Employee evaluations include level of knowledge & demonstrated capabilities • Training expands beyond an individual's specific job responsibilities to develop a broader "system-level" understanding of why they do what they do • Incidents and near-misses lead to real changes, not just observations
Questioning Attitude	All employees constantly ask themselves what might go wrong. They anticipate potential problems and are alert to unusual conditions. They don't assume, they verify.	• Risk mgmt. is collaborative v. combative and continuous v. static • Risk mgmt. strategy assumes mistakes will occur and puts controls in place to prevent and/or detect issues early • Employees ask questions & escalate when things don't seem right
Integrity	People can be relied upon to support the team by doing the right thing, the right way, every time, whether someone is looking or not.	• Management systems are formalized (i.e., procedures & controls are maintained, defined, known and certified) • Role- and level-specific expectations are set and communicated at each level; performance is evaluated during employee reviews • Feedback is specific and timely (i.e., daily, weekly)
Active Team Back-up	All employees actively back each other up. They act as 'each others keeper' by looking for what might be wrong or was missed in another's area while expecting the same in return.	• Operational & Execution Vulnerabilities (OEVs) are defined, documented, maintained, and widely known • Critical items receive more human oversight (not less)—multi-person integrity for high-risk tasks

The HRO Pillars enable an environment of Operational Discipline



Operational Discipline is:

"Doing the right thing, the right way, every time"

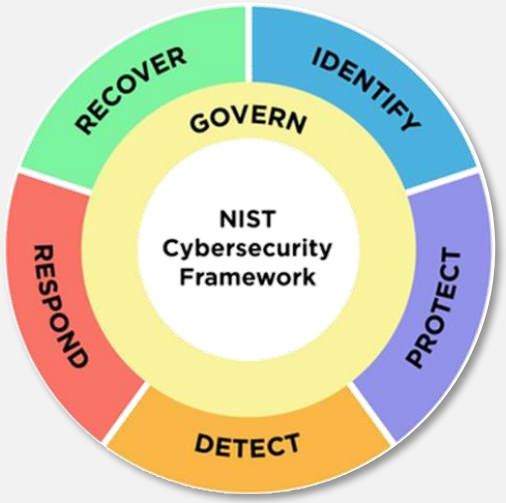
This is easy to say, but very hard to do, especially in a complex operating environment

Operational Discipline and the HRO Principles are essential to effective cybersecurity

Traditional IT management processes and systems must evolve to integrate, reinforce, and sustain HRO Principles

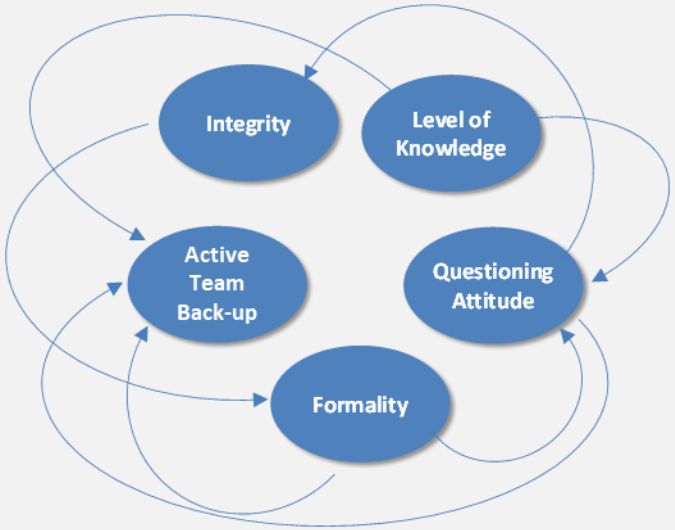
TRADITIONAL CYBERSECURITY FRAMEWORKS

Cybersecurity frameworks (e.g., NIST CSF 2.0) are necessary but **insufficient** on their own. They fail to align work practices to the values of HROs, increasing cyber risk related to human error.



HIGH RELIABILITY PRINCIPLES

All high-performing organizations share a set of common operational traits. The Pillars guide **behaviors** and **ways of working** at every level and for every role in the organization.



WP&C'S INTEGRATED MANAGEMENT SYSTEM

We embed HRO Pillars across management systems, enabling **proactive identification** and **response to risks** (cyber and otherwise) while executing established controls with operational discipline.

1	Leadership	Committed Leadership defines and communicates vision and metrics; robust cultural elements in place
2	Employee Accountability	Employees know what they are accountable for, take ownership, and receive frequent feedback
3	Risk Identification	With clear vision, priorities, roles and accountabilities in place, risks to successful execution are identified
4	Risk Control	Once risks are identified and assessed, the means for controlling them are put in place
5	Knowledge Sharing	Knowledge is collected, synthesized, and incorporated across the organization
6	Management of Change	Processes are clearly defined and controlled so that change can be managed effectively
7	Continuous Improvement	Assess compliance and effectiveness of controls; performance steadily improves; the system learns

Becoming a High Reliability Cyber (HRC) organization is a journey, and significant capability gains are made at each level

Level 1: **Defined**

- HRC Pillars are defined
- Role-specific expectations are set & communicated

Level 2: **Measured**

- A system measures HRC Pillars & behaviors
- Current and desired HRC behaviors are defined—interventions are developed to close gaps

Level 3: **Managed**

- HRC Pillars and operating practices are actively managed
- Managers at all levels understand and manage to HRC fundamentals
- Incident management includes a review of whether HRC has broken down or an unrecognized risk needs to be mitigated

Level 4: **Integrated**

- HRC obj. are integrated into Mgmt. Systems
- Employee performance includes evaluation of alignment with HRC
- HRC Pillars & behaviors are embedded in hiring
- Orientation & upkeep programs stress the HRC Pillars and behaviors

HRC MATURITY

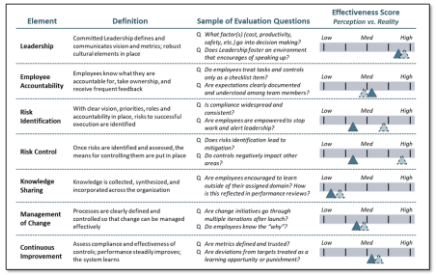
The benefits realized at lower levels of maturity generate momentum that enables dedicated management practices without adding large resource requirements

WP&C's proven tools and approaches accelerate and de-risk your transformation to a High Reliability Cyber Organization

Yardstyck® HRC Assessment

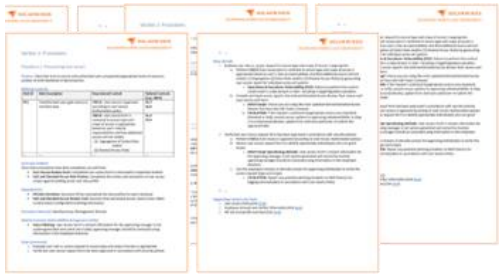
WP&C's proprietary tool that enables you to measure, quantify, and benchmark your operational values and behaviors against HROs

Cyber-Management System Evaluation



Assesses the effectiveness of your Cyber-Management System to create a prioritized (based on risk and benefit) improvement roadmap

HRC Process Runbooks



HRC Runbooks are highly effective operations manuals that take a 'systems-view' to account for process and system dependencies, embedding HRO prompts to drive better execution of core processes

LEADS HRO Transformation Path

WP&C's proven approach guides organizations through HRO transformations—driving performance improvements from the start of the effort

Measure how well you leverage the power of your people in the fight against cyber attacks—take our 12-question self-assessment

www.wilsonperumal.com/cyber-assessment

Learn more about IT Complexity and High Reliability Cybersecurity

READ OUR UPCOMING CYBERSECURITY PUBLICATION

Cybersecurity Complexity Survey & Report

How Complexity is Endangering the Transition to ZTNA

Release: June 2024

Upon publication, you will be able to access the report here: www.wilsonperumal.com/ztna-complexity-report

WATCH OUR MOST RECENT EXECUTIVE WEBINAR

IT Complexity

The Reason your ZTNA Implementation is Likely to Fail, Just like Many Digital Transformations

www.wilsonperumal.com/webinars

Watch our on-demand WP&C Executive Webinar

CONTACT
ERNIE SPENCE

CONTACT
DEAN HAMILTON