Wilson Perumal & Company
EXECUTIVE WEBINARS

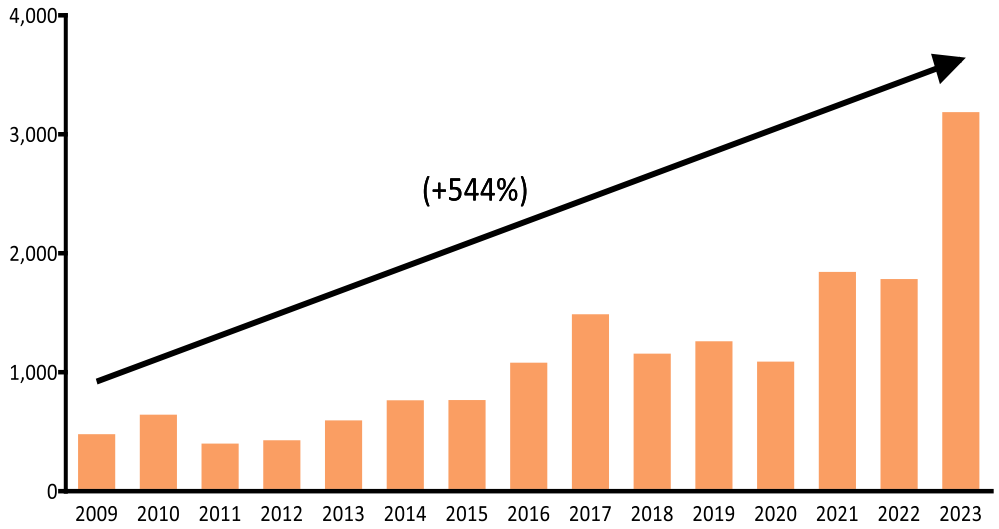
IT COMPLEXITY:

The reason your ZTNA implementation is likely to fail, just like many digital transformations

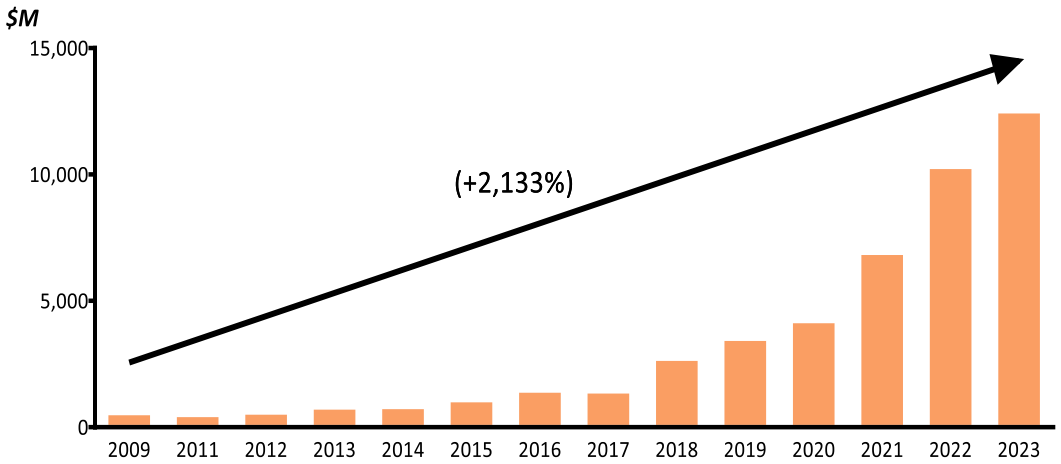
WATCH THE WEBINAR

Our traditional approach to cybersecurity has failed—and IT complexity is a major cause of that failure!

ANNUAL CYBER ATTACKS IN THE U.S.



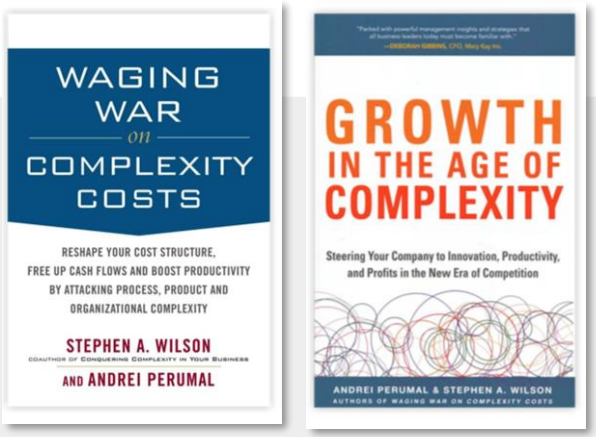
ANNUAL AMOUNT OF MONETARY DAMAGE CAUSED BY REPORTED CYBERCRIME IN THE U.S.



In 2023, the world spent $223B on cybersecurity technology and services to defend against cyber crime

Source: Identity Theft Resource Center, FBI Internet Crime Report

There is a clear link between IT complexity and cybersecurity risk



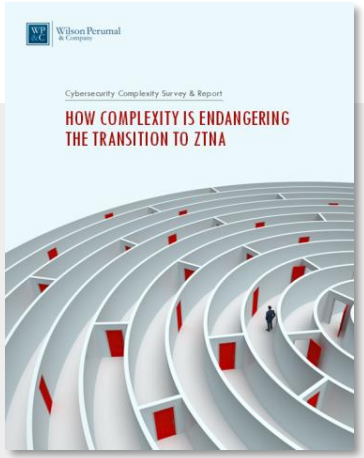
We wrote the book on complexity.

(Two, in fact!)

Human errors increase in complex environments

We have unique insights into improving human performance in complex environments

Human performance can be drastically improved



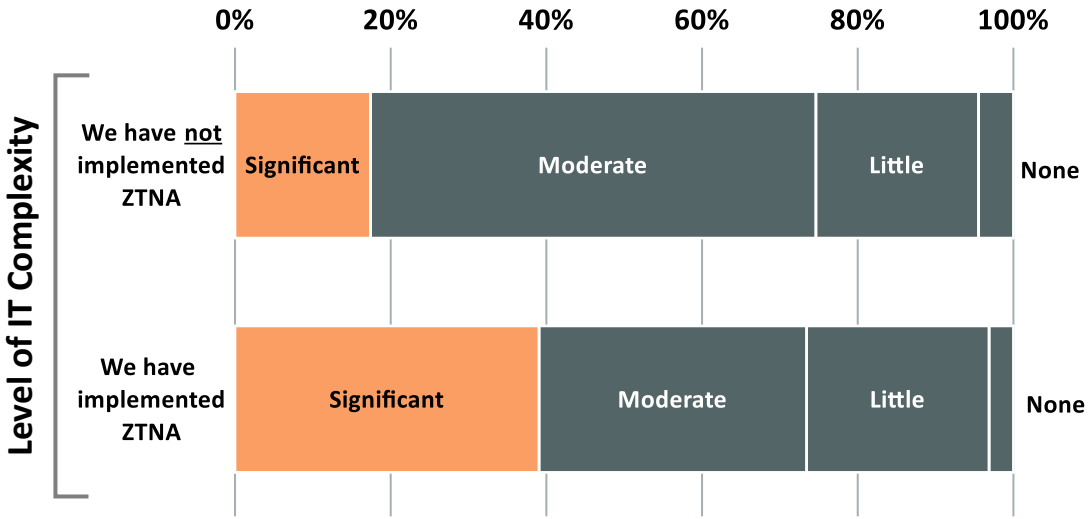
We conducted a first-of-it's-kind study to explore the effects of complexity on cybersecurity and ZTNA

Our new research indicates that ZTNA may fall victim to unaddressed IT complexity

Our primary research indicates that ZTNA also drives complexity and cost

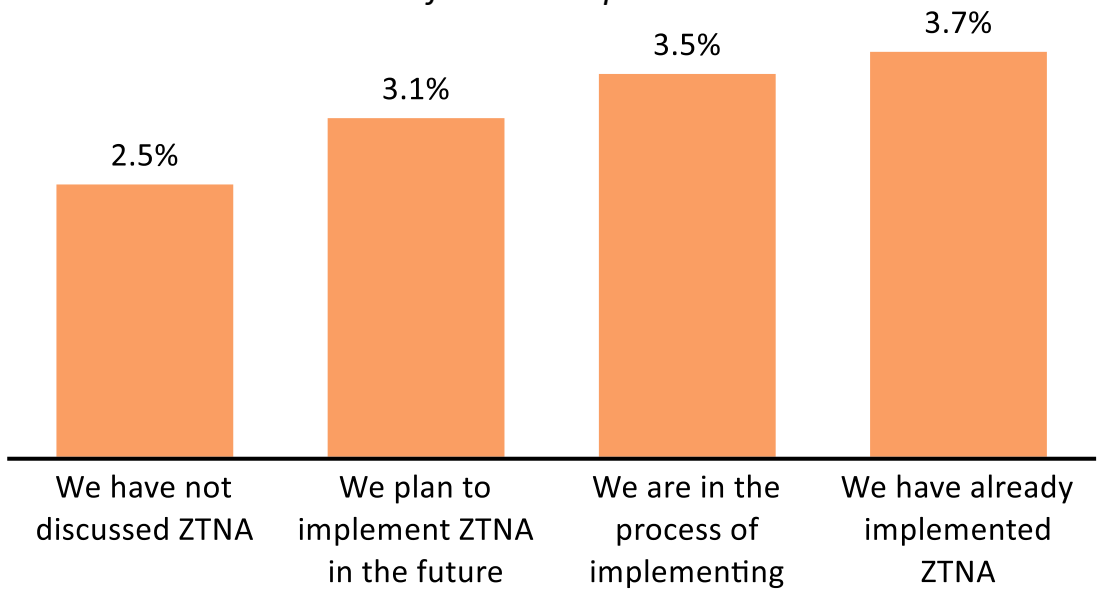
ZTNA ADDS SIGNIFICANT IT COMPLEXITY

40% of tech leaders that have implemented ZTNA say it adds "Significant" complexity to their IT Operations



ZTNA SIGNIFICANTLY INCREASES IT SPENDING

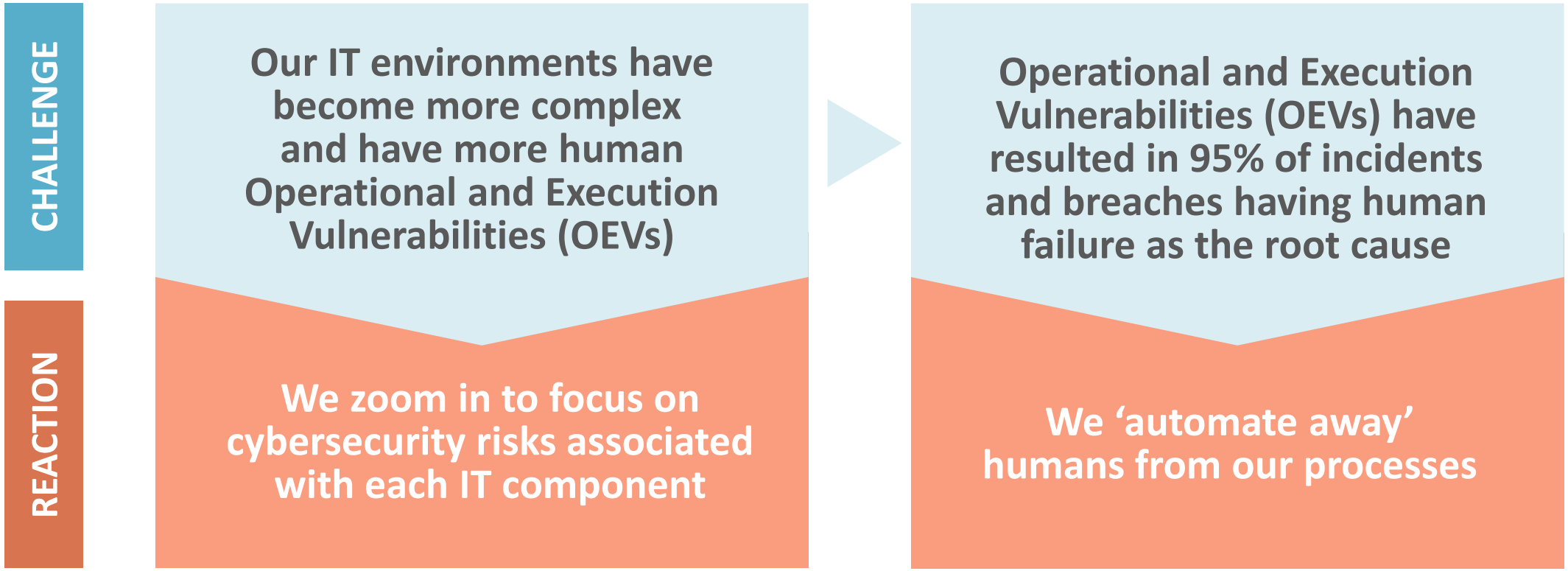
IT spending increases (as a % of revenue) over the course of a ZTNA implementation



ZTNA implementations are also failing 'quietly'—the percentage of organizations saying they fully implemented ZTNA dropped from 40% to 28% between 2021 and 2023

Source: WP&C ZTNA Survey, Fortinet

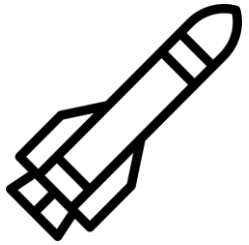
Cybersecurity leaders are aware of complexity-related challenges, but their natural reactions only make the problem worse



These reactions make sense for "complicated systems" **but not for "complex systems"**

Source: World Economic Forum

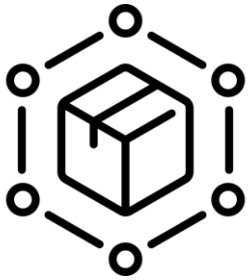
We use the word "complex," but we react as if we mean "complicated" *(it is critical to know the difference)*



COMPLICATED SYSTEMS

Example: *Unmanned Rocket*

- Can be decomposed and understood as individual parts
- Behaviors are linear and deterministic
- Can be reliably modeled by combining parts
- Can be effectively automated



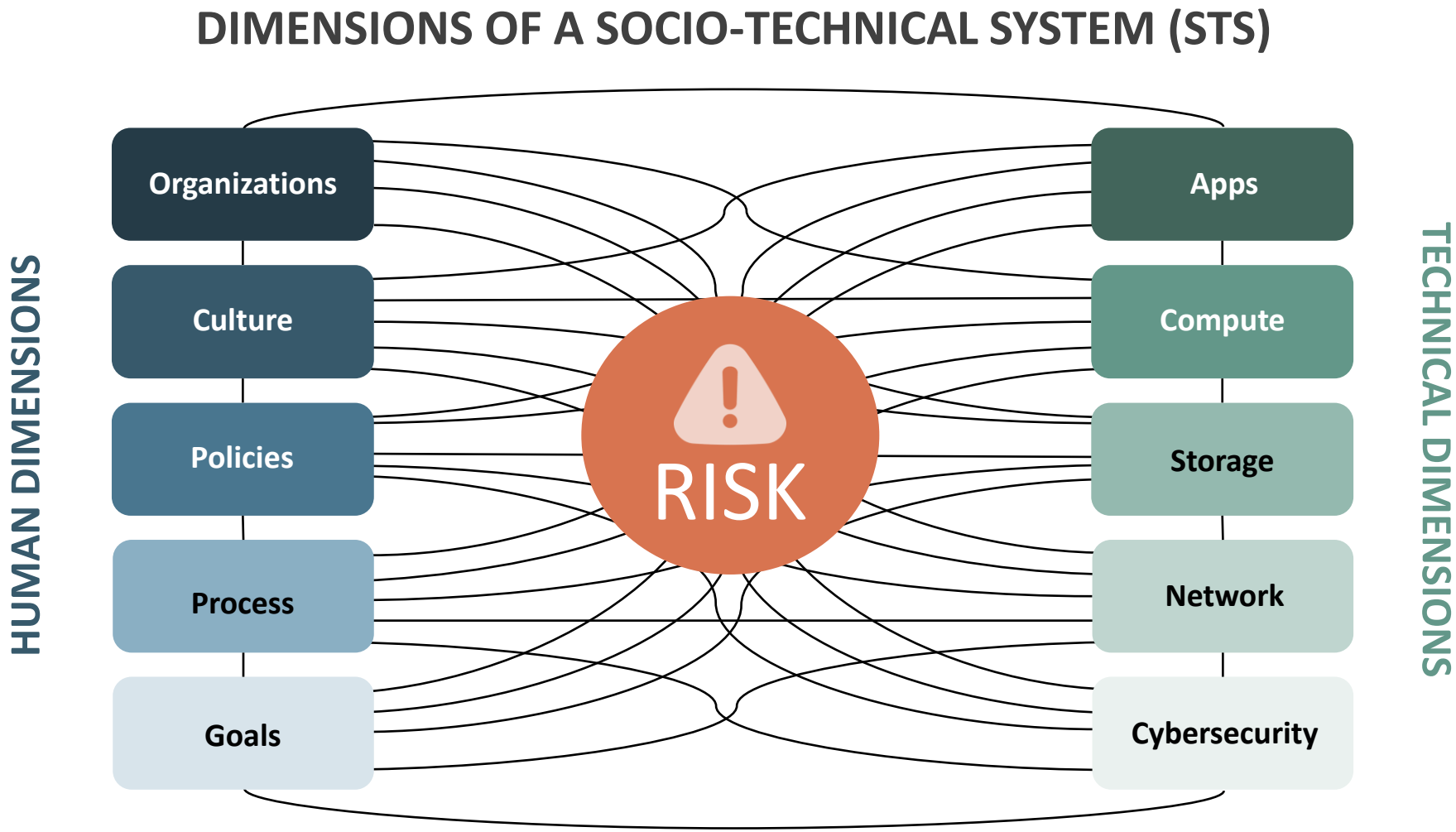
COMPLEX SYSTEMS

Example: *Supply Chains*

- Can only be understood by looking at the entire system
- Behaviors are nonlinear and chaotic
- Modeling can provide a false sense of security
- Cannot be fully automated

You cannot safely manage risk in **complex** systems
using tools meant for managing **complicated** systems

IT environments are "socio-technical systems" which are highly complex and, therefore, highly unpredictable and risky

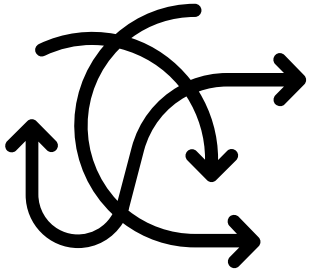


Source: Zimmerman, Renaud; *International Journal of Human-Computer Studies*

People have an advantage over machines in risky and unpredictable types of environments

HUMANS ARE DESIGNED TO EXPLORE THE UNKNOWN

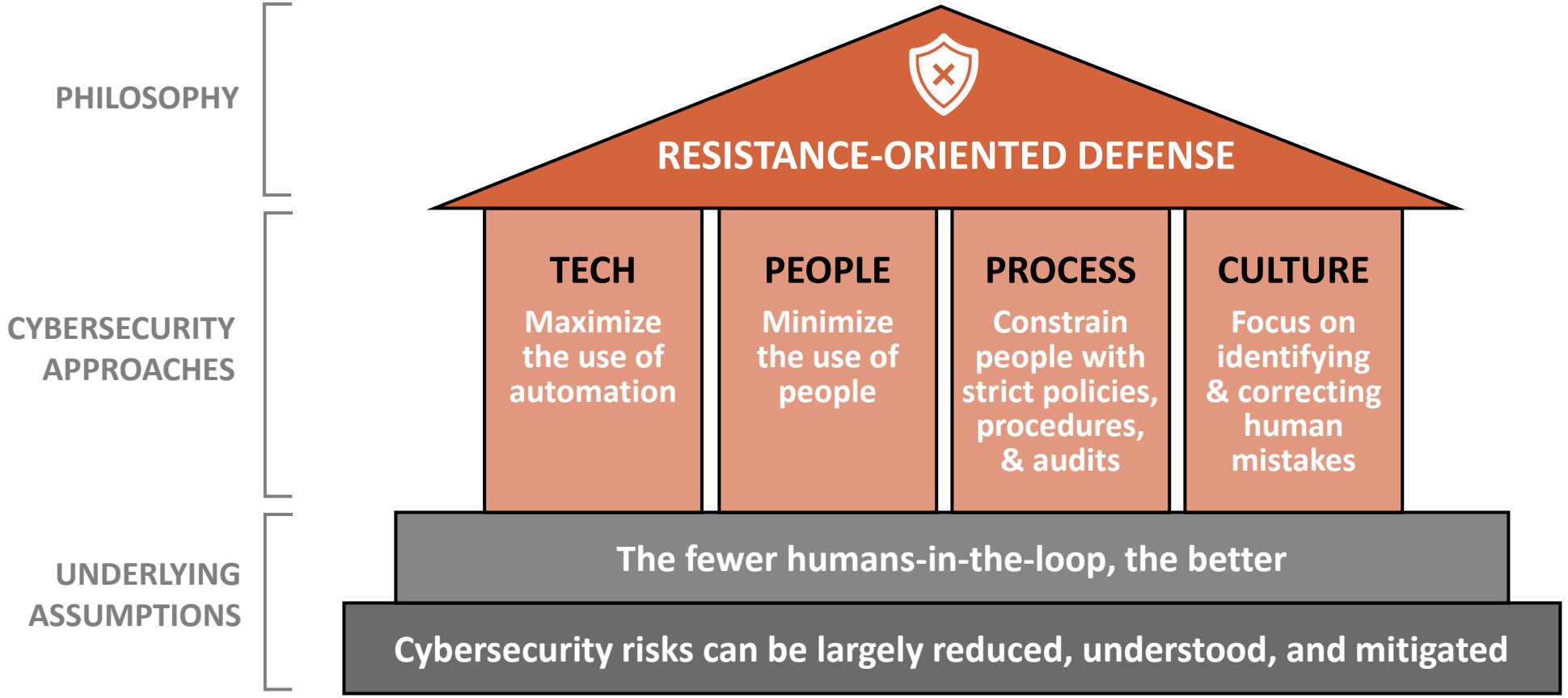
We are better than machines at **reasoning about the implications** of things we haven't seen before



We are more **creative**, **adaptable,** and make better decisions in **dynamic** and **unpredictable** environments

To reduce IT cybersecurity risk, **focus on people and process**—not just technology

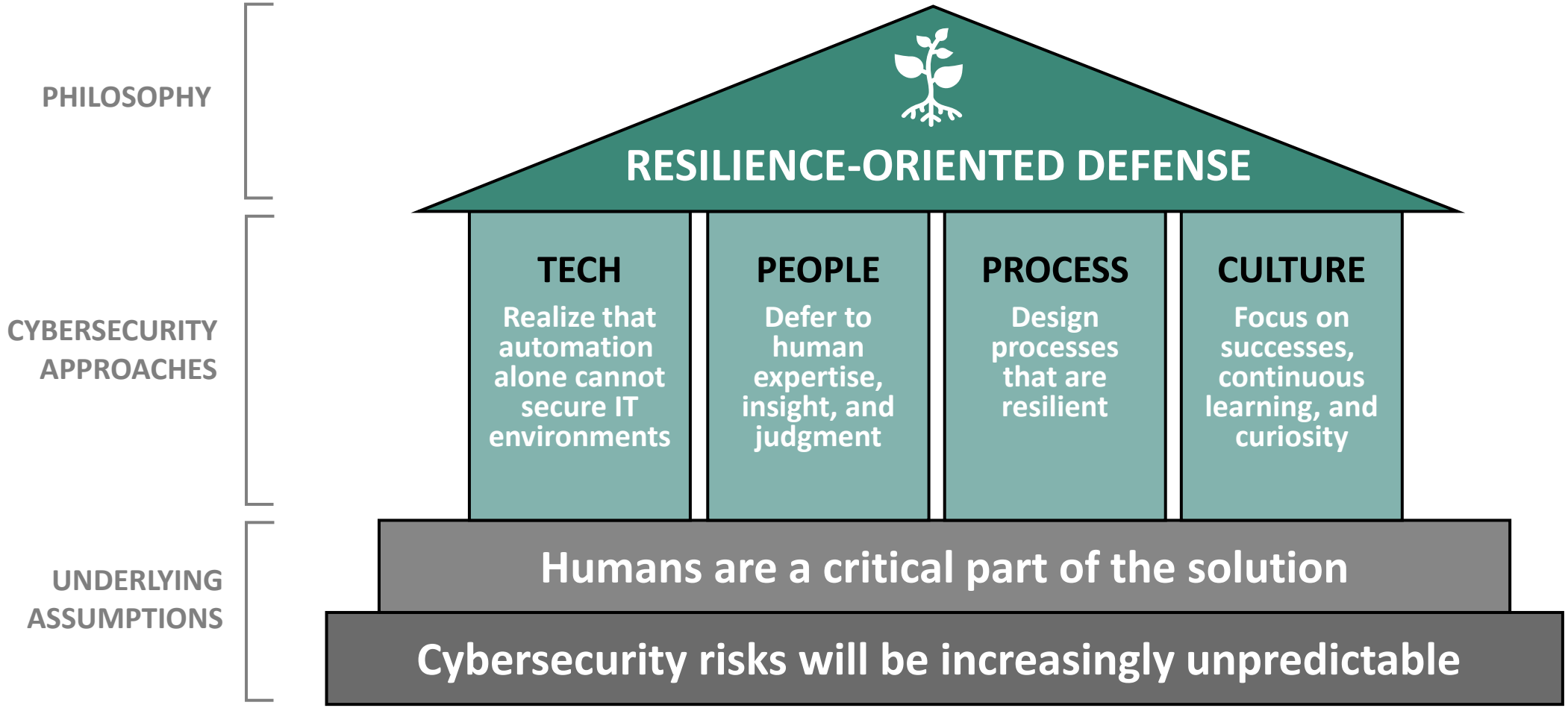
This misunderstanding has led to our failed *"resistance-oriented"* approach to cybersecurity



This approach may work for complicated systems, **but not for complex systems**

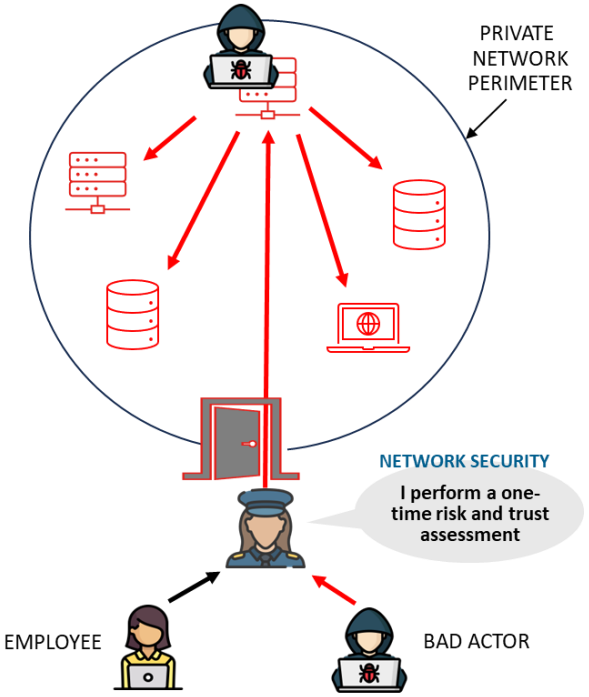
Source: Zimmerman, Renaud; *International Journal of Human-Computer Studies*

Alternatively, a *"resilience-oriented"* approach leverages technology while also taking advantage of the inherent strengths of people

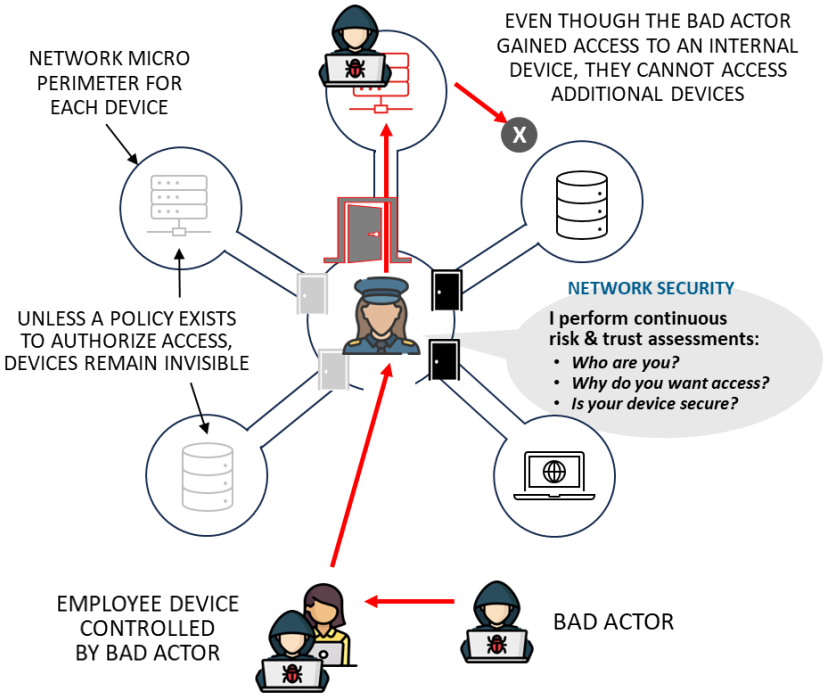


ZTNA is not a technology (like VPN)—it is an entirely new and complex operational paradigm

The legacy perimeter-based security model assumes that all devices inside a firm's network can be trusted



No matter how strong your security is, if a bad actor gets in through an external door, they can spread out laterally and vertically



ZTNA assumes the bad actor has already gained access to the network and does not allow freedom of movement across devices

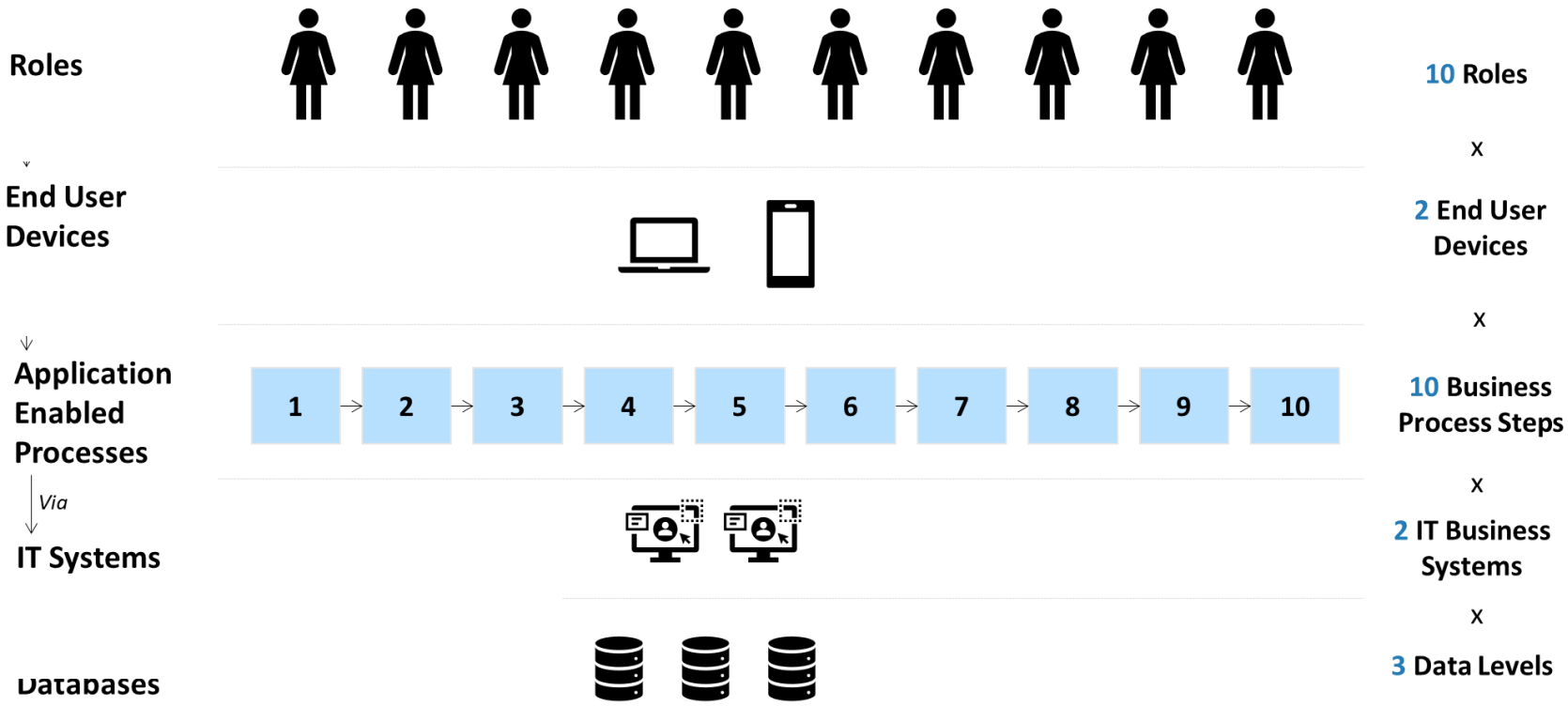
Zero Trust Network Access (ZTNA) assumes no devices can be trusted and checks every device before it's granted access to another device

At its most extreme, ZTNA requires explicit and unique policies for every permutation

CASE STUDY:

ZTNA COMPLEXITY IN A SMALL END-TO-END BUSINESS PROCESS

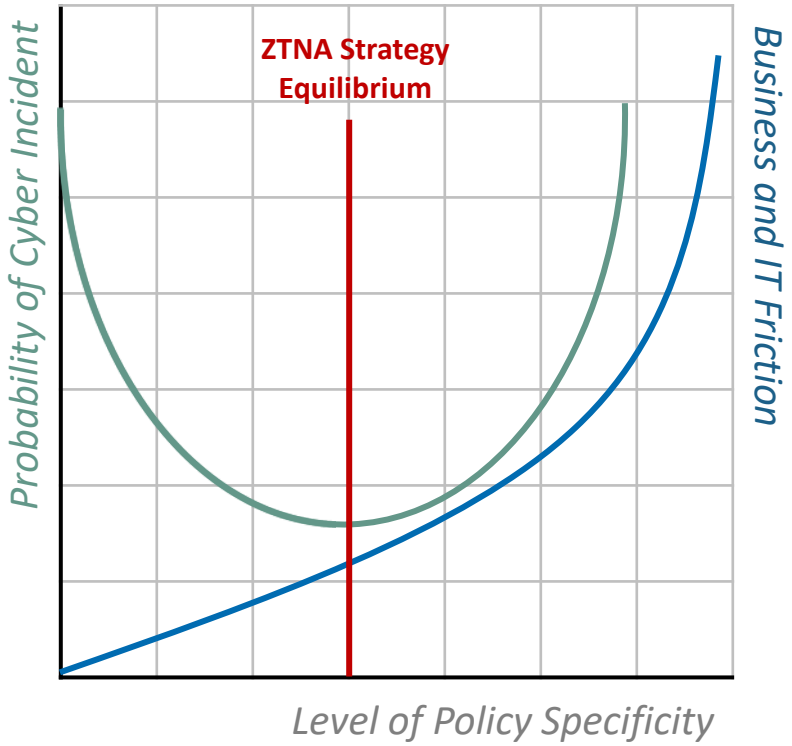
Up to 1,200 potential ZTNA policies may have to be considered



Practical ZTNA requires a compromise:
the right equilibrium is what determines if ZTNA helps you or hurts you

ZTNA requires so much process complexity that it could actually impair business efficiency and *increase cybersecurity risk*

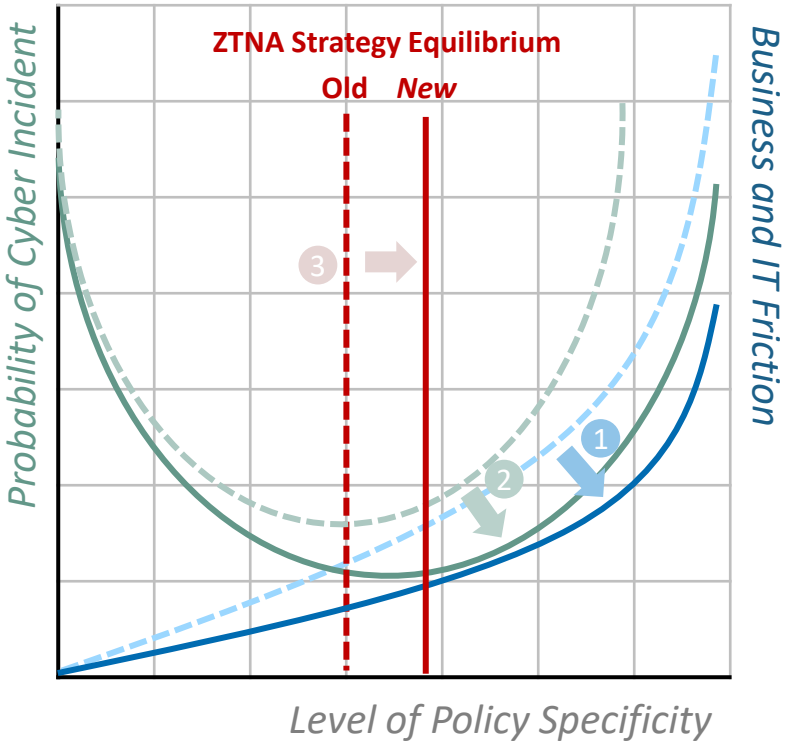
Balancing ZTNA Strategy v. Business Impact



Tighter scope of trust can increase cybersecurity effectiveness (to a point)

This tightening introduces process and end-user friction—resulting in workarounds, shortcuts, and increased probability of a cyber incident

Reducing Friction to Improve Cyber Performance

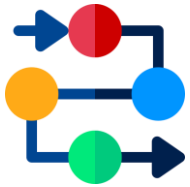


To move the equilibrium, an organization must address process and human factors that result in higher rates of friction 1

This flattens the probability curve 2

Resulting in a new equilibrium 3

WP&C's High Reliability Cybersecurity (HRC) methodology incorporates resilience-oriented practices into ZTNA implementation



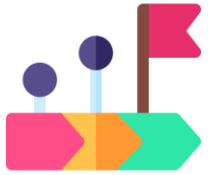
Identify and assess ZTNA pilot area of focus

Develop HRC Runbooks (with OEV* mitigations) for change management

Stand up HRC multi-functional pilot team and propose initial ZTNA policies

Set up HRC Operational Excellence Management System (OEMS)

Evaluate policies against Enterprise Architecture for complexity risks



Go-live with pilot, build enterprise roadmap, incorporate learnings, and rollout to other BUs

Learn how to implement **High Reliability in cybersecurity** in our next webinar, June 14th

*OEV = Operational and Execution Vulnerabilities; OEVs identify weaknesses in human processes

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

ATTEND OUR NEXT EXECUTIVE WEBINAR

People are Assets, Not Threats:
The Missing Piece of Your Cybersecurity Strategy

Friday, June 14th at 12 PM CST
Register: www.wilsonperumal.com/webinars

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 the IT Complexity WP&C Executive Webinar

CONTACT
DEAN HAMILTON

CONTACT
ERNIE SPENCE