adair

The blind spot of cybersecurity. Now illuminated.

The challenge

Hackers today are more con artists than malicious nerds. They spend less time probing networks than probing teams: they focus on human weakness because technical weakness has become rare. They impersonate co-workers, stage false urgency to provoke impulsiveness, orchestrate distractions to avoid detection, or groom frustrated teams as co-conspirators.

The cybersecurity market is attempting to counter these attacks by training teams to be more knowledgeable about threats, to be more alert during digital interactions and to have safe devices at hand. They focus on knowledge, on awareness, and resources.

But even the most aware, well-trained, and best equipped teams will fall prey to social hacking when they're distracted, fatigued or chasing a tight deadline.

The solution

High consequence industries like medicine, nuclear power or aerospace have mastered human risks for decades – in a depth that is not yet mastered by cybersecurity experts.

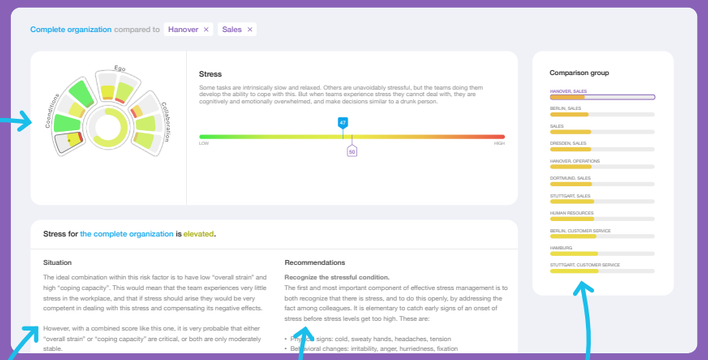
Whenever the consequences of failure are catastrophically high, the gold standard for managing human risk are the "Dirty Dozen" human factors. They originate in the airline industry, but can be applied to any activity with a critical human risk component.

All twelve have been the subject of thorough scrutiny and continuously studied, validated and refined.

They can be influenced by leveraging behavioral metrics, human factors research and computational sociology – the fields we're experts in.

All wrapped up in a modern and accessible tool.

It **measures and visualizes team realities** that are relevant for cybersecurity...



... **explains in detail** what they mean and what their impact is...

... and then provides clear, pragmatic and highly effective **instructions** on how to **shape** them.

Team by **team**.

The Dirty Dozen

Managing these well-researched twelve human risk factors forms the backbone of operations at almost all armed forces, at NASA, at Airbus, at the NHS and at the CDC. They were a core part of the worldwide response to Covid-19.

Three of these twelve risk factors are already being addressed in cybersecurity: knowledge, awareness and resources. The remaining nine are no less critical and adair provides the means to understand and control them.

Lack of **Knowledge**

Lack of **Awareness**

Lack of **Resources**

adair reveals both the problem and the solution

Based on an eight-minute sociological survey, adair reliably calculates and indicates the probability of secure behavior of every team in your organization.

It shows both what the problem is and what the proven ways are to control it. You don't just get a fancy metric showing you where you're at: adair tells you what you can do to improve.

Objective – reliable – solution oriented.

Lack of **communication**

When teams aren't encouraged to speak freely or fear repercussions for sharing their thoughts, crucial information doesn't flow properly. Instructions and situations become unclear and subject to interpretation, creating an easily exploitable illusion of agreement and clarity.

Complacency

Complacency is a core influence on secure behavior since it is either a complete failure to detect an error or an unacceptably slow response to it.

Distraction

Working humans think ahead; the probability to skip a few steps when distracted during work is very high. A well-timed distraction is therefore one of the main tools of social engineering.

Lack of **teamwork**

When the outcome of tasks is a shared responsibility, any misunderstanding regarding who does what massively impact not only productivity but also security. Hackers need only one unsupervised process step to wreak havoc.

Fatigue

Exhaustion is like suffocation: you can't compensate for lost rest by resting more later, just like you can't make up for not breathing by breathing more later. A fatigued team isn't merely slower, it's dumber: it fails to apply even basic skills and knowledge, not to mention common sense.

Pressure

When the pressure to meet a deadline interferes with the ability to complete tasks correctly, secure behavior becomes impossible. Security compromises abound and the securing of assets shifts lower and lower in a team's priorities.

Lack of **assertiveness**

When teams notice something unusual or irritating, or discover a weakness no one seems to grasp, it is not only up to management to hear them, but up to the teams to bring sufficient attention to it.

Norms

Numerous processes don't run the way they were designed and implemented, but the way it's "always been done", because it's comfortable and supposedly more streamlined. Such informal processes tend to be invisible to cybersecurity audits and constitute a serious loophole for bad actors.

Stress

Some tasks are intrinsically slow and relaxed. Others are unavoidably stressful, but the teams doing them develop the ability to cope with this. But when teams experience stress they cannot deal with, they are cognitively and emotionally overwhelmed, and make decisions similar to a drunk person.

www.adair.app
info@adair.app

adair GmbH
Zum Röthepfuhl 1
14974 Ludwigsfelde