MITSloan Management Review

DIGITAL RESILIENCE

The Unaddressed Gap in Cybersecurity: Human Performance

High-reliability cybersecurity operations leverage human performance as a critical layer of defense.

Stephen A. Wilson, Dean Hamilton, and Scott Stallbaum

An employee at Maersk, the world's largest shipping conglomerate, saw computer screens suddenly turn black and irreversibly lock in late June 2017. A highly engineered malware worm exploited company computers in Ukraine lacking the latest Microsoft Windows security patches. With this small foothold, the worm breached the company's IT system and blocked access to all computers and servers worldwide, ultimately halting shipping operations for several days. The incident cost Maersk over $200 million in lost revenue, caused unquantified costs in perished goods and recovery efforts, and created a slew of unhappy customers.

The Maersk story is not uncommon. In 2015, 80 million customer records were stolen from Anthem because an unsuspecting employee responded to a phishing email. In 2017, the United Kingdom's National Health Service suffered a ransomware attack that resulted in 19,000 canceled appointments due to the use of, once again, an outdated, unpatched version of Microsoft Windows. In 2019, data on 106 million Capital One customers was stolen via a misconfigured Amazon Web Services firewall. And the list goes on.

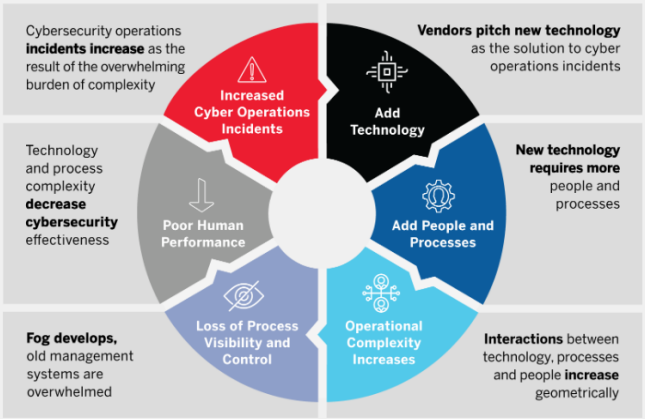
With cybersecurity high on the corporate agenda, falling victim to a catastrophic breach is the dreaded nightmare scenario. Amid the COVID-19 crisis and a sudden increase in remote work arrangements, cybercrime is surging. Boards are looking to CEOs to prevent cyber incidents — but how?

"More advanced technology" is a common answer, but even that would not have prevented the Maersk incident, where a small human oversight — not installing a software update — led to catastrophic consequences. Technology is clearly the focus of industry investment and such spending is forecast to be $133 billion per year by 2022. But while choosing the right technology is essential, the majority of incidents relate to gaps in human performance, a persistent and often overlooked cybersecurity issue in most organizations.

Without addressing this issue of human performance, a vicious cycle perpetuates. (See "A Technology-Led Cycle Leads to Increased Cybersecurity Incidents.") As companies bring on board new technologies — each one potentially addressing an emerging threat — they also add more corresponding people and processes. As this continues, the interactions between technology, processes, and people pile up, and the level of complexity increases geometrically. At some point, this complexity overwhelms the cybersecurity infrastructure and obscures emerging threats — until, weighed down by legacy systems, the business finds itself less agile than cybercriminals, and an attack occurs. In response, the business seeks out the technological patch for that specific threat, and the cycle repeats.

A Technology-Led Cycle Leads to Increased Cybersecurity Incidents

Adding discrete processes and technologies can create an overwhelming burden of complexity and decrease cybersecurity effectiveness.



Enter the High-Reliability Cybersecurity Operation

Closing the human performance gap — embedding new behaviors and shared understanding as part of the culture and normal course of business — is no small undertaking, but it's ultimately the best defense against cyberattacks. And fortunately, an analog exists for addressing this type of risk and leveraging human performance as a critical layer of defense: the high-reliability organization (HRO), which we define as an organization that has a remarkably low number of mishaps consistently over a sustained period of time yet performs highly complex and inherently hazardous tasks.

The HRO concept stemmed from practices that originated more than 60 years ago with the United States' Naval Nuclear Propulsion Program, which recognized that unique organizational practices were needed to put a highly complex nuclear reactor on a boat, under the ocean, and operate it safely with a crew of young sailors. This meant eschewing the traditional military culture that had existed for centuries: Follow orders, do what you're told, and don't ask questions. Following NASA's loss of the space shuttle *Columbia*, the *Columbia* Accident Investigation Board looked to the United States' nuclear navy as the preeminent model for a high-reliability organization. HRO ideas later gained prominence as part of the energy industry's response to growing complexity and catastrophes such as the *Deepwater Horizon* disaster and then spread to the health care, manufacturing, and now cybersecurity fields.

HROs are different from non-HROs in three specific ways:

- **Mindfulness.** HROs exhibit *chronic unease* — a state of hypervigilance and watchfulness for early danger signals.
- **Responsiveness.** HROs identify emerging issues early and respond quickly to arrest the development of the incident.
- **Learning capacity.** HROs learn from every event and quickly disseminate knowledge to rapidly improve the system. (In the U.S.'s nuclear navy, this means that every submarine that goes to sea represents the cumulative lessons of over 6,200 years of reactor plant operations.)

These characteristics of an HRO have been well studied and well characterized in academia, but less well understood are the *pillars of the program* — the individual operational pillars that, when enacted, collectively result in an HRO's superior performance. These pillars are *formality*, *level of knowledge*, *integrity*, *questioning attitude*, and *active team backup*. We have focused on the pillars in our research while developing a mechanism for measuring a company's alignment with HRO characteristics.

High-reliability cybersecurity operations (HRCOs) employ these same HRO pillars to close the human performance gap and add a critical, additional layer of cybersecurity. Long gone are the days where cybersecurity was solely the responsibility of the IT department — cybersecurity is now everyone's business. The table "HRO Pillars and Their Application in Cybersecurity" further describes each HRO pillar and how it can be applied in HRCOs.

HRO Pillars and Their Application in Cybersecurity

Applying the five pillars of high-reliability organizations can help an organization become a high-reliability cybersecurity operation.

HRO PILLAR	DESCRIPTION	EXAMPLE APPLICATION IN HRCOS
Formality	• People follow authorized procedures (not workarounds). • They communicate in a disciplined manner to ensure information is consistent and reliable.	• Processes are in place to manage privileged identities, accounts, and information. • Rules are clear for why privilege is conferred, who is responsible, and how it is reviewed.
Level of Knowledge	• People understand not only what they do but why they do it. • They continually expand their understanding of systems, processes, and hazards around them.	• Users understand how easily passwords can be compromised and the risk of unauthorized access. • Everyone uses unique strong passwords and password vaults and supports periodic password changes.
Integrity	• People can be relied upon to do what they say they will and what is expected of them. • They hold themselves and others accountable.	• Employees willingly operate within security policies and use tools as designed/intended. • They do so even if it changes how they do their work (using company-provided devices, limiting downloads or access, regular backups, etc.).
Questioning Attitude	• People anticipate problems and are alert to unusual conditions. • They ask: What could go wrong? What has changed? What might I or others be missing?	• Given the limitations of antivirus filters, employees have a chronic unease about the validity of emails. • Employees check URLs prior to clicking on links and are suspicious of requests for personally identifiable information.
Active Team Backup	• People actively look out for one another. • They understand they are part of something larger than themselves and must work in concert to be effective.	• When configuring new firewall access, team members cross-check/test the updates. • They do so in a planned and structured manner — not out of mistrust but to provide a check to ensure completeness and accuracy.

Let's consider what an HRCO looks like in practice. Everyone in an HRCO has a high *level of knowledge*. They understand how easily passwords can be compromised and the risks of unauthorized access; because they recognize that cybersecurity is everyone's job, they read and take seriously the warnings that the cybersecurity department sends out each week. There is a level of *formality* in how security processes are managed — a clear protocol for managing privileged accounts and information, which only works when coupled with *integrity*, the willingness to operate within security protocols even if personally inconvenient. This formality also highlights when something is out of place or out of the ordinary, enabling a *questioning attitude* that keeps employees from clicking on an email or questionable URL that looks suspiciously like a phishing attack. Finally, people in an HRCO always have each other's backs — *active team backup* — so when configuring new firewall access, team members cross-check and test the updates, not out of mistrust but to provide a check on completeness and accuracy.

These pillars can be effected by each individual in the organization and therefore serve as the basis for helping it transform into an HRCO. While cultures are often described in aggregated or descriptive terms, impacting individual behaviors is the only way you can truly *move* a culture.

The first step is to develop a baseline understanding of how individuals view the culture around them and what they deem to be their ideal *target culture*. If there are looming gaps in how a culture currently performs, but there exists strong organizational alignment about how a culture aims to transform, then the battle is half won. Conversely, if front-line workers and senior management have very different views of what is ideal, then it will be hard to move to HRCO practices until that dissonance is resolved.

In our research, we assess a company's alignment with HRCO pillars by having individuals rank a group of 40 cultural descriptors by best fit. Each descriptor — "do what you're told," "anticipate problems," "pay attention to hierarchy" — is a simple phrase that corresponds to one of the five pillars and has been honed to tease out to what degree an organization acts like an HRCO. This analysis yields a quantitative assessment of its cultural alignment with HRCOs — a critical insight into what is traditionally a data-free area of study. Such an analysis helps it understand the behaviors that represent the greatest source of potential risk, the parts of the business that bear these potential risks, and the organization's alignment to HRCO principles by level and role.

It's worth noting that some descriptors reflect behaviors that on the surface seem "right" but can actually undermine the resiliency of an HRCO. For example, when employees are expected to "be results-oriented" and/or "do whatever it takes," they aim to deliver great outcomes and be rewarded for it. But these behaviors can lead to workarounds (counter to formality) and going "outside the system" (counter to integrity). Similarly, superiors who tell their teams to "bring solutions, not problems" may intend to encourage employees to proactively solve problems and take ownership, but in practice this solution-focused mindset discourages them from quickly alerting others to an issue (counter to having a questioning attitude).

The cybersecurity community is awakening to the yawning gap in human performance. In February 2020, "the human element" was the central theme for a major cybersecurity conference. The key emerging ideas were familiar: Technology alone is insufficient; things are changing too quickly; we need to tap organizational practices as a key additional line of defense.

Even the best technology will fail or become obsolete in the face of ever more sophisticated hacks. The billions spent on cybersecurity technology have not, and will not, solve the problem. Strong protocols and procedures are imperative but cannot account for every scenario. We recommend that managers turn to the lessons of HROs — organizations that have been able to operate in decentralized, high-risk environments, with a remarkably low number of incidents — and begin their journey to becoming an HRCO.

Ultimately, inculcating HRCO behaviors offers an irreplaceable benefit: When technology and process fail, human performance is all that stands between you and a cyberattack.

ABOUT THE AUTHORS

Stephen A. Wilson is cofounder and managing partner at consulting firm Wilson Perumal & Company (WP&C). Dean Hamilton (@hamildean) is chief technology officer and partner at WP&C, and Scott Stallbaum is a manager there.