Principled Leadership:
A Case for Enterprise-wide Artificial Intelligence (AI)

Introduction

> "*The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty and we must rise with the occasion. As our case is new, we must think anew and act anew. We must disenthrall ourselves, and then we shall save our country.*"
>
> — Abraham Lincoln

The purpose of this scenario is twofold:

1. Introduce 15 Enterprise AI Principles that function as a blueprint for enterprise-wide AI operating systems, including rationale and implications for each principle.
2. Embed the 15 Principles in a generic futuristic story; a scenario that puts the principles in context so senior leaders can better understand threats and opportunities to public and private organizations.

In the wake of one of the most sophisticated and perhaps largest hacks in more than five years of several government agencies, and the fact we were unaware of these attacks until recent weeks, is reason enough to refute any notion that the "status quo" with respect to cyber and artificial intelligence is acceptable. Something must change. To paraphrase Abraham Lincoln, "as our case is new, we must think and act anew". Here is a scenario which the authors hope will help leaders understand the stakes and the need for action "with all deliberate speed".

In his brief called "Organic Design for Command and Control", the father of the OODA loop and F-16 USAF Colonel John Boyd came to the conclusion that a better title would be "Appreciation and Leadership".

His definitions:

Appreciation - refers to the recognition of worth or value, clear perception, understanding, comprehension, discernment, etc.

Leadership - implies the art of inspiring people to enthusiastically take action toward the achievement of uncommon goals.

The authors of the following scenario (Mr. Mark Montgomery and Dr. Robert Neilson) have elected to use a single scenario just for simplicity sake to begin a strategic dialogue with CEOs and their teams[i]. It is our earnest hope that chief executives will appreciate the value of the ideas and technology this scenario is bringing forward, and exert the leadership necessary to "inspire people to enthusiastically take action toward the achievement of uncommon goals". It is also our earnest hope the ideas and technology presented in this scenario will encourage executives to exert the leadership necessary to remain competitive and thrive in the era of artificial intelligence.

Vice-Admiral James P. "Phil" Wisecup (Ret.)

It is May, 2021. Cynthia Robinson was promoted to CEO of Resilient, Inc., a Fortune 100 company, during the second wave of the pandemic in 2020 when her long-time mentor decided to retire. She had worked her way up through multiple business units after returning to her alma mater for her MBA twenty-three years ago. Cynthia was the first female CEO and the youngest CEO in the 100-year history of the company.

What is the KYield OS?

The KYield OS is a distributed artificial intelligence operating system based on the theorem 'Yield Management of Knowledge' developed by Mark Montgomery in his applied lab in 1997. The core of the AI OS is patented.

Unlike other types of operating systems, the KYield OS provides governance over distributed networks. The system is enhanced by artificial intelligence, providing precision augmentation tailored to each individual, team and business unit.

Embedded functionality includes prevention of crises, proprietary security, and enhanced productivity. The AI OS works in the background with a simple to use natural language interface with apps tailored for each entity.

End Goal:

Create an efficient Continually Adaptive Learning Organization (CALO) with the KYield OS to minimize global risks and maximize opportunities.

Day 1: It was 6:41 a.m. on Tuesday, May 11th. Cynthia was having breakfast on her deck overlooking the Atlantic Ocean when she received an urgent text on her phone from Trevor, head of cyber security (CISO) for Resilient: "We may have a serious problem. Call me asap."

Trevor rarely contacted her this early, so Cynthia decided to call him on her way to the office and put him on speaker phone. "Hi Trevor, what's up?" Trevor responded, "You remember the digital supply chain disaster last year?" Cynthia responded, "Yes, of course, how could I forget it?" "Well," said Trevor, "we thought we had it contained in January, but it looks like it was just the beginning" … "our entire supply chain may be compromised." Cynthia responded "xxxx, just what we don't need. Brief me in an hour in my office—and have your team get started on a presentation. We may have to call an emergency board meeting."

By 8:45 a.m., Trevor had fully briefed Cynthia and several others on what appeared to have the potential to be the worst crisis in the company's history. Trevor hosted a confidential discussion group with CISOs from their large global ecosystem and had discovered that a key supplier of Resilient was testing a new distributed AI system that alerted to unusual data activity in their supply chain, so the supplier's CISO investigated. He was able to trace the anomaly back to Resilient. It appeared that a trojan horse application had been installed in their office suite software, and was using the cloud to propagate the malware throughout the digital supply chain. The malware was sharing data with companies worldwide that were also unaware of the breach, but the final destination had yet to be confirmed.

KYield Enterprise AI (EAI) Principles

Principle 1: *EAI should have governance, ethics, and security built-in from inception.*

Principle 2: *Design-in systemic data quality management.*

Principle 3: *Maintain strong security.*

Principle 4: *Embed integrity throughout AI systems.*

Principle 5: *Maintain objectivity.*

Principle 6: *Provide privacy, transparency and explainability.*

Principle 7: *Empower individuals.*

Principle 8: *Adopt enterprise-wide architecture.*

Principle 9: *Turbocharge prevention with EAI.*

Principle 10: *Accelerate discovery and productivity.*

Principle 11: *Establish and maintain a competitive advantage.*

Principle 12: *Leverage EAI for continuous human learning and improved decision making.*

Principle 13: *Mitigate risk in development, auditing, and monitoring EAI.*

Principle 14: *Incentivize accuracy and improvement with knowledge capital.*

Principle 15: *Continuously adapt.*

Day 2: The CISO group held an emergency video call to discuss the situation. The early consensus was that the malware was installed during the breach in 2020, and had likely been transferring critical data ever since.

Day 4: Cynthia called an emergency meeting for her management team and board for 8 a.m. on Friday morning, the 14th of May. Most of the individuals were working remotely worldwide, so the call was held in the board room with video conferencing. After a briefing from Cynthia and Trevor, the chairman of the board asked "How did we get in this trap, and how do we get out of it?" The Chief Risk Officer (CRO) responded that digital supply chain risk has been warned about for years, but few listened and left it up to vendors to sort out. She continued to describe how this event was viewed by CROs as continuance of the 2020 digital supply chain breach, probably by the same state actor.

Cynthia then asked "What's the worst they can do to us?" Trevor responded, "So far it appears to be intel collection and espionage, but it could turn into an attack at any time." He said that the state actor could shut down their global digital operations, hold their systems for ransom, or manipulate data for whatever purpose they desired. He concluded by saying, "With control over the productivity suite and cloud infrastructure, they can do just about anything they want."

After considerable silence, the chairman asked, "Why is so much of our business operation dependent on a single vendor?" Everyone looked at Jim, the CIO, who replied, "Remember our report for the annual board meeting in February of 2020? We recommended adopting a multi-cloud strategy with less reliance on a few large vendors." Jim then described how the consulting firm advising the company recommended expanding the relationship with the giant software vendor, including consolidation of the company's datacenters to the software vendor's cloud.

The CRO interrupted, “The larger the vendor, the greater the risk.” The chairman asked why the consulting firm made such a recommendation and three of the senior managers replied in unison, “They are strategic partners.” Cynthia called an end to the meeting with instructions to her team to find solutions and report back at 8 a.m. Tuesday morning.

Day 5: Cynthia called her tech leaders Saturday morning to learn more, and discovered from Jim that the AI company that found the data anomaly had been sending him articles and papers on AI for years. She then recalled reading articles from the company. Jim said that he had talked to the founder and attempted to convince Cynthia’s predecessor to pilot their system, but he wasn’t strong in tech and didn’t seem comfortable taking risks with small companies, so typically followed the advice of consultants.

Apparently, the vendor had been working on AI systems for decades and wasn’t considered a ‘cybersecurity’ company, though multiple security methods were embedded in the system. Jim said the AI system was the only one of its kind he was aware of. Similar to the malware, the AI OS was distributed; installed across the enterprise for each entity. The vendor’s research demonstrated that while one-off AI projects were easier to fund, enterprise-wide AI systems were essential. Jim described how the founder experienced a eureka moment following an especially intense period in the lab when he realized that multiple functions within the system working interactively with precision data were necessary to achieve critical functionality, without which none would function well.

> *“In the case of all things which have several parts and*
> *in which the totality is not, as it were, a mere heap, but*
> *the whole is something besides the parts, there is a cause;*
> *for even in bodies contact is the cause of unity in some cases,*
> *and in others viscosity or some other such quality.”* — Aristotle [ii]

Principle 8: *Adopt enterprise-wide architecture.*

Rationale: Value sometimes arises where least expected.

Implications: The one individual or sensor left out of EAI for the enterprise, supply chain, or ecosystem might be the one that recognized and alerted an existential risk.

Principle 2: *Design-in systemic data quality management*

Rationale: AI systems are only as good as the data they train on.

Implications: Garbage-in / garbage-out; quality-in / quality-out.

Principle 3: *Maintain strong security*

Rationale: EAI includes the most important human workflow in the enterprise, including strategy, planning, and intellectual property.

Implications: Compromised EAI systems can be devastating to the organization.

Cynthia said, “Sounds impressive, but how would such a system have prevented this type of sophisticated breach?” Jim replied, “We can’t be certain—no system is perfect, but prevention of crisis is their core specialty and one of several functions embedded in the distributed AI OS. Their system did find the anomaly when billions of dollars previously invested failed. If it had been installed when I first recommended, we might not be in this position.”

The next person Cynthia called was their CTO, Jan, who had a Ph.D. in Computer Science from Carnegie Mellon[iii]. Cynthia had leaned on Jan quite a bit since becoming CEO. Jan answered her phone, “Hi Cynthia, let me guess—calling about the cybersecurity problem?” “Yes”, said Cynthia, “It’s like a recurring nightmare that just won’t go away. I need you to brief me on the technology the company used that found the anomaly.”

Jan replied, “We looked at them last year before Jim recommended it. The functions in the AI OS have been proven elsewhere. However, it’s the only unified system I am aware of. They have been working on this for decades and appear to be years ahead of anyone else.” Cynthia asked Tina, “Jim said it wasn’t a cybersecurity company—what else does the system do?”

Principle 4: *Embed integrity throughout AI systems*

Rationale: Enterprise-wide AI systems interacts with the entire organization, providing a foundation for integrity.

Implications: If the AI systems lack integrity, so too will the organization.

“Enterprise-wide learning, prevention, and productivity. It may seem strange in an IT vendor”, said Jan, “but it’s common to include security in products. We provide many functions in some of our products. Think about the auto industry—safety and security are embedded in all new product designs to work as a single unified system. Although unusual in the computer industry, particularly for small companies, ‘systems of integrity’ is not a new concept in engineering. We’ve seen more focus on integrity engineering in the last twenty years due to 9/11, the financial crisis, BP oil spill, auto emissions fraud, Wells Fargo sales scandal, the COVID pandemic, and the SolarWinds trojan horse.” After a pause, Jan concluded “We obviously need to focus more on cybersecurity.”

Principle 1: *EAI should have governance, ethics, and security built-in from inception*

Rationale: Good system design is paramount. Governance is the foundation AI systems are built upon.

Implications: Attempting to add-on governance, ethics, and security after the fact is technically difficult, inefficient, and prone to error.

Principle 6: *Provide transparency and explainability*

Rationale: In order to earn and maintain trust, EAI systems should be transparent and explainable in a simple manner.

Implications: If employees, customers, and partners don't trust the system, they are less likely to participate and/or attempt to work around the system.

Principle 10: *Accelerate discovery and productivity.*

Rationale: Well-designed AI systems have a unique capacity to augment, enhance, and accelerate discovery, R&D, and execution.

Implications: May not be possible to catch competitors that more effectively apply EAI to productivity growth and R&D.

Cynthia asked, "So what does this AI OS look like—is it similar to anything we are using?" Jan replied, "It's a modular system with a natural language interface, so it's a bit like productivity, email or social networking on steroids." Cynthia said, "Sounds easy enough—not much training then?" Jan continued, "Not for individuals, but certification is required for senior admins. I pulled up the paper they sent us… let's see—there it is. They have a CKO Engine, which is like a semi-automated chief knowledge officer bot. It provides governance for the entire system—access, levels of security, and ethics." Cynthia responded, "some of our largest shareholders are asking about AI ethics—legal and compliance expects regulation soon". Jan said, "Agreed, and with good reason. I hope they do more good than harm. It looks like this AI OS was designed with governance in mind."

Cynthia continued, "We have a lot of stakeholders worried about big brother. How do they get buy-in? Is this legal in the EU?" Jan responded, "We'd need to loop in our compliance people to confirm, but their data management appears consistent with EU regulations. They embrace privacy and provide a prominent link in navigation so individuals can check anytime to see what algorithms are being used and why."

Jan described the other functions in the AI OS, including more on security methods, prevention, and enhanced productivity. Jan was familiar with the deep learning and genetic algorithms the system used, and she wanted to test for accelerating R&D across business units, but they lacked the data structure, AI system, and software applications. Like most of their peers in the Fortune 100, Resilient was still performing one-off AI projects and integrating machine learning in their own products. They didn't have anything resembling an enterprise-wide AI OS. Although the company had dozens of Ph.Ds. in CS and hundreds of software engineers, they were focused on their core business. Jan explained that the cost is minimal when spread across many companies. Cynthia asked Jan to check into it further and brief the team during Tuesday's management meeting.

Principle 9: *Turbocharge prevention with EAI.*

Rationale: The highest ROI possible is prevention of major crises.

Implications: Failure to prevent crises can lead to a negative spiral, failure, and collapse.

Principle 13: *Mitigate risk in development, auditing, and monitoring EAI.*

Rationale: How and who designs, audits, and monitors AI systems can determine the outcome.

Implications: A significant percentage of large enterprise crises have been due to internal actors ("don't try this at home").

Day 6: On Sunday morning, Cynthia called her CRO Tom, "Hi Tom, sorry to bother you on a Sunday morning. I need to get my head around this digital supply chain crisis." Tom said, "No problem, Cynthia, what can I do for you?" Cynthia continued: "I'm trying to quantify the damage and understand the risk moving forward, and what can be done to resolve it. Tom said, "I'll have an initial risk assessment in 24 hours." Cynthia replied, "Thanks. What do you know about the company that found the anomaly in our supplier?"

Tom replied, "I became interested in the company a couple of years ago when they announced a program called 'HumCat', which stands for prevention of human-caused catastrophes[iv]. It's loosely patterned after 'nat cats' for natural catastrophes, but focused on humans and organizations." Cynthia asked, "How does the prevention work?" "Well," Tom said, "Jan can fill you in on the technology, but my understanding is that the AI OS picks up most of the anomalies from employee work flow. People in organizations inevitably warn about an impending crisis, it just gets lost in the bureaucracy." Cynthia said, "I've seen that enough in my career". Tom responded, "Haven't we all. These types of systems have deep intelligence across enterprise networks that can process enormous amounts of information—far more than we can. The AI OS can pick up anomalies that would be impossible in an organization the size of ours otherwise."

Cynthia asked Tom, "Have any of your peers developed these systems in-house?" Tom replied, "I'm aware of a couple, but I wouldn't advise it. Whether malintent, accident, or ignored warnings, the majority of major crises have been caused or enabled by internal actors. After the fact, cover-ups are the norm rather than exception." "We've run into that problem all-too-often," said Cynthia, "I suppose it's best to restrict these types of systems to a small group of external experts with tight security, whose job is in part to protect organizations from themselves."

Principle 5: *Maintain objectivity.*

Rationale: AI systems are an invitation for manipulation from political activists, fraud, and governments with totalitarian tendencies, resulting in misinformation or even dystopia. Unless prevented, unconscious bias can also become embedded in AI through human workflow and algorithms.

Implications: Maintaining objectivity in EAI is essential. Cognitive bias is a significant risk in AI systems that has already been realized at scale.

The two then discussed the need for objectivity, agreeing that no individual career is worth existential risk in a large crisis like the one they were currently facing, observing that most senior teams are replaced after large preventable crises.

Day 7: Monday, May 17th, was the most difficult day for Cynthia since she became CEO. Her day was orchestrated primarily by their crisis management team with back-to-back calls with customers and suppliers. Word about the crisis had also been leaked to the press, so the PR team kicked into high gear, and the company's stock had dropped 13%. Stress levels had increased exponentially. After the last conference call, Cynthia texted her EA, Nancy, to ask Bob to meet her at a waterfront restaurant. Bob was Resilient's long-time chief counsel and close friend to Cynthia and her mentor, Doug, the company's former CEO and her predecessor.

"Hi Bob, thanks for coming down to chat", said Cynthia, "it's been quite a week." "So I've heard—I read the story in the WSJ this afternoon," Bob replied, "what's the latest?". Cynthia briefed Bob on the situation and discussions with her team, then asked Bob: "Do you know why Doug didn't embrace more advanced technology? The vendor our supplier used that found the breach is the same vendor our tech team recommended to Doug last year, but he declined and went with the consultant's recommendation. If we would have adopted that system, we may have uncovered this mess months earlier, if not prevented altogether." Bob paused, then said, "That's why you are CEO".

Bob explained that their generation didn't grow up with technology, and neither he or Doug had sufficient expertise to make informed decisions, so they just followed what others were doing. Bob said, "We are all aware of the conflicts between consultants and big tech companies, and that most of the innovation that provides us with an advantage comes from small companies—that's why we acquire several a year on average."

What is the Synthetic Genius Machine (SGM)?

The SGM is newer patent-pending invention by KYield's founder, Mark Montgomery (2019). The SGM is a resulting from the last decade of R&D. Much of the research in the SGM was conducted from 2009-2016 when Mark was a frequent guest and contributor at the Santa Fe Institute.

As the name implies, the SGM combines the work products of human geniuses with synthetic computing to deliver an interactive genius bot for deep specialties. The component technologies include identifying and capturing knowledge patterns and features, and a new symbolic language, which serves to provide multipurpose functionality, including greater efficiency and encryption.

The SGM is pre-optimized for AI systems and quantum computing. It is designed for efficiency at the confluence of AI and quantum in preparation for integration of the two types of high-performance computing as they evolve.

The SGM can be run independently or combined with the KYield OS.

He concluded, "When a mistake like this comes up, we just blame the consultants. Eventually, everyone on the board, including Doug, realized that technology had become so important for the business that it was time to bring in a younger, more tech savvy CEO." Cynthia spent the last few years as President of Asia, so wasn't in the loop on most of these discussions. It all made more sense to her now after talking to Bob.

Day 8: Cynthia started her day on Tuesday, May 18th, with a run along the beach as the sun was rising. Although she was saddened that her old friend and mentor failed to prevent this crisis—neither had the government, big tech, or any of their peers. She wasn't about to let this crisis damage her mentor's legacy, their company, or her future. She asked her driver to pick her up at home so she could prepare for the management meeting at 8 a.m. on the way to the office.

Cynthia opened the meeting by stating, "We need to quantify the actual risk to the company, determine the best path forward, and make sure this doesn't happen again. Jan, please start us off with a briefing on what you've found. Technology got us in this mess—maybe it can get us out of it."

"Thanks, Cynthia," Jan said, "The bad news is that we don't know if this is the end of it or not. Our teams have isolated the malware and removed the source of the current problem. However, the compromised digital supply chain last year provided the perfect opportunity for one of the world's top state-sponsored cyber hackers to place time bombs across our network. This may be the beginning of the end of this event, or it may be the end of the beginning—we just don't know." Jan continued, "The good news is that it may not matter, at least with our most important workflow. We've been looking at options to fix this problem for the short-term and the long-term. This is a video presentation from the founder of the company that detected the anomaly, which alerted us to this problem[v]."

Principle 12: *Leverage EAI for continuous human learning and improved decision making.*

Rationale: Rapid machine learning only becomes an advantage when it improves human behavior.

Implications: Failing to rapidly learn in the AI era risks extinction.

Principle 11: *Establish and maintain a competitive advantage.*

Rationale: AI systems learn quickly, innovation is accelerating, and the gap between AI leaders and laggards is rapidly expanding.

Implications: Organizations that fail to maintain competitive AI systems are at high-risk of falling behind, disruption, and displacement.

Jan showed the group a clip of the founder at a conference discussing a new genius machine that included a new symbolic language. Jan and his team had devised a plan to collaborate with the vendor to accelerate the development of the symbolic language and apply it to the AI OS. The founder agreed by email that this would allow Resilient to convert its workflow to highly efficient encrypted data that would be very difficult for anyone to break. In addition, he recommended random variations of the language with keys physically delivered by armed security guards. So if the state actors had sleeper apps in their networks, and in the unlikely event broke the encryption with quantum computing, the language and keys would change frequently on a random basis.

Cynthia said, "I like the sound of that—it would mitigate our risk moving forward. How long would it take to get up and running?" Jim, the CIO replied, "In our discussions last year they said it would require about six months, but they've come up with a method to accelerate the process. We can discuss it further, but I think they can probably get a limited system up in a few weeks that would begin protecting our most sensitive workflow, and expand from there. Our people say the symbolic language will take time to mature and complete, but we've already started using multiple types of encryption, so we think any espionage on new work products and communications is minimal to nonexistent."

Jan continued, "Once initiated, the AI OS enhances the learning for every entity where it's installed—all business units, teams, and individuals, and it learns rapidly." Jim said, "This was our primary reasoning for our recommendation last year—it should provide us with an ongoing advantage. None of our direct competitors have installed this system yet."

Cynthia asked Resilient's well respected head of human resources, Linda, to review the vendor's material and attend the meeting. Cynthia asked, "Linda, what do you think the impact would be on our culture and

workforce if we installed this enterprise-wide AI OS?" Linda responded, "We would want to monitor closely and retain the ability to make changes as necessary, but the system offers a couple of positives from an HR perspective. Although the governance is unified, it reflects legal and compliance realities, and has the ability to tailor to local jurisdictions. Despite many subsidiaries and business units, a unified culture is necessary—we should be on the same team with the same organizational mission, provided we encourage creativity and healthy competition. The individual modules in the AI OS are tailored to the needs of each individual, and appear to do so in a trustworthy manner, which is critically important. If the system finds a potentially serious internal security risk, our security team would conduct an investigation in the same confidential manner we do today—a compliant manner. Cynthia responded to Linda, "What do you think about this knowledge capital?"

Principle 7: *Empower individuals; including privacy.*

Rationale: Organizations of every size and type consist of individuals.

Implications: Organizations that lose sight of the needs of individuals experience low morale, high turn-over, and cultural deterioration.

"We've seen a few companies attempt something similar," Linda said, "but none I'm aware of have been widely adopted by our peers". Linda continued, "The information collected in this AI system on the workflow must be considerably more than we collect now to provide those functions, so it seems plausible they could provide more accurate incentives. If we go in this direction, my advice would be to start with psychological incentives first and then test financial incentives with a small work group. If we can better align our reward system with individuals and the goals of the business units, it may help attract and retain top talent, particularly in areas of competitive talent wars, like AI where big tech dominates."

Principle 14: *Incentivize accuracy and improvement with knowledge capital.*

Rationale: Data intelligence within the system allows more accurate financial and psychological rewards with digital currency, which can serve to guide organizational and individual behavior.

Implications: Organizations that fail to recognize and reward top performers tend to lose them to competitors.

Resilient's CFO, Carol, interjected, "Remember a few years ago when Berkshire Hathaway reduced their investment in us? In private discussions, they said they thought our incentive programs weren't competitive".

> *"I think I've been in the top 5 per cent of my age cohort all my life in understanding the power of incentives, and all my life I've underestimated it."* — Charlie Munger

Day 10: Cynthia was undergoing deep soul searching during her run along the ocean on Thursday morning. She had long observed CEOs following a pattern of attempting to find 'plausible deniability' just to be found guilty in the eye of stakeholders. At what point did state sponsored cyber warfare switch from plausible deniability to culpable deniability for private sector CEOs? Like it or not, it appeared that cyberwars and retribution between nation states was now her responsibility. As she pulled her car out of the garage, Cynthia decided it was time to call her old friend and mentor, Doug, who was also her predecessor.

"To what do I owe the pleasure, Cynthia," Doug said, "something to do with cyber security?" "Good guess, Doug," Cynthia replied, "I can see why you decided to retire". Doug asked, "Is it as bad as it sounds?". "We're not entirely sure yet," replied Cynthia, "but it's not good." She continued, "I wanted to talk to you about a possible solution. You remember that AI OS Jim recommended last year?" "Sure," Doug replied, "what do you need to know?". Cynthia then told Doug that it was the same system that discovered the anomaly in their supplier for the ongoing crisis.

"I've talked to the team about it," Cynthia said, "but I'm wondering why you didn't move forward with a pilot?" Ah, that's simple, Cynthia, "I was getting ready to retire, it represented a big long-term strategic shift for the company, and I wanted you to be able to make that decision, so I punted." Cynthia said thanks, I think…" Doug continued, "What I liked best about the system was the concept of continuous learning and adaptability across the enterprise. The board realized Resilient wasn't adapting fast enough to changing conditions, and we agreed it was time for a new CEO, but I wasn't confident enough to make that call on your behalf. I wasn't sure if you would want to buy, build, or might find something else. I just thought it was better for the new CEO to make such strategic decisions." Cynthia said, "I really appreciate the background," Doug, "Let's get together for coffee in a couple of weeks and I'll fill you in on my decision."

Principle 15: *Continuously adapt.*

Rationale: "The species that survives is the one that is able best to adapt and adjust to the changing environment in which it finds itself." – Charles Darwin, *The Origin of Species*.

Implications: The pace of change appears to be accelerating. Organizational cultures that master AI systems for continuous adaptation are most likely to thrive in the future.

Author Bios

Mark Montgomery is the founder and CEO of KYield, Inc. He is originator of the theorem 'yield management of knowledge', and inventor of the now patented AI system KYield OS, and patent-pending Synthetic Genius Machine. Mark was a frequent guest and participant at the Santa Fe Institute from 2009-2016. His articles have been published in books, journals, *Wired*, and *Computerworld*.

Vice-Admiral James P. "Phil" Wisecup (Ret.) is a member of the KYield board of directors. Phil graduated from the U.S. Naval Academy in 1977. In 2008 he became the 52nd President of the US Naval War College and left active duty in 2013 as the Inspector General of the US Navy after 36 years of service and three commands at sea, including the USS Ronald Reagan carrier strike group. He was Director of the White House situation room, held senior posts in Europe and Asia, and upon leaving active duty was appointed as Director of the CNO Strategic Studies Group.

Dr. Robert E. Neilson is a member of the KYield board of directors. He was a senior KM Advisor to the Army's CIO/G-6. Formerly, he was the Chief Knowledge Officer, department chair and a professor at National Defense University. Rob has taught in the U.S. and internationally, and has published books and articles on topics ranging from cyber ops to organizational learning. His futuristic scenarios have been featured in "*The Futurist*".

Day 12: Cynthia pushed hard on her morning run to achieve her time goal, thinking about how to turn this mess around from a negative to a positive. In the final mile of the run, she wondered if an enterprise-wide AI OS would help Resilient compete with two of the big tech companies that were beginning to displace them in core markets. She decided on her sprint to the finish that it was time to make a bold decision. As she was walking back towards her house to cool off, she sent an email to Nancy on her smart watch, "Set up a call with the founder of the AI OS firm ASAP".

Nancy greeted Cynthia at the elevator with a cup of decaf and said, "I've got the guy on the phone—just pick up when you're ready to talk to him". After introductions, Cynthia asked the founder, "How sure are you this AI OS of yours will work the way you expect it in a company like Resilient?" "We can expect hick-ups along the way—always are," the founder said, "but technical viability was resolved quite some time ago." Cynthia responded, "I've been briefed on why we didn't adopt the system last year—had nothing to do with your company, but I'm curious why others haven't".

The founder replied, "It's a long, difficult trek across the valley of death in the commercialization of revolutionary technology, and it's full of minefields. If I had to sum it up in one sentence, it would be a combination of timing, matchmaking, and leadership. In hindsight, several of your peers should have adopted that didn't and the result was a major crisis our systems would have likely prevented. It's the most frustrating part of this business."

Cynthia said, "Well, we have a problem, my team thinks your AI OS may be the solution, and the timing is yesterday. We are all taking significant risks here, but I think it's necessary. Let's set up a video conference with our tech team and come up with an emergency action plan." The founder replied, "Sounds good." Cynthia continued, "I expect you and your team to be there for us every step of the way, and we want a fair price." The founder replied, "That's all we've ever asked for. You have my full support."

Epilogue

The scenario presented above paints a vivid picture of a security breach in the private sector. No organization is immune from insidious cyber-attacks when connected to accessible global networks, nor is continued success guaranteed. Indeed, organizations that fail to proactively seek continuous improvement and competitive advantages with advanced technologies are often "*swept off the historical stage overnight",* as Putin warned, published by TASS just four days before the FireEye blog announcing detection of the Russian-linked SolarWinds hack.

The increasing sophistication of cyber-attacks experienced in 2020 is consistent with the long-term trajectory of state actors and industrial espionage. We expect attacks in all environments will be increasingly intelligent, autonomous, and adaptive at speeds beyond the ability of traditional cybersecurity defenses to contain, essentially requiring distributed AI systems for an effective defense. A distributed AI OS designed with precision can provide the competitive foundation across the enterprise, upon which all other functions will increasingly depend, including individual learning, worker productivity, discovery, innovation, intelligence, strategic planning and global operations.

Embracing the 15 Enterprise AI Principles provides an enterprise-wide framework for the global enterprise. Licensing and deploying the KYield OS with rules-based governance will result in an executable system with the 15 Enterprise AI Principles and specific functions embedded across the enterprise, supported by consulting from decades of theoretical and applied R&D.

Our research indicates that from this point forward, the fate of organizations and perhaps countries will be substantially dependent upon the structural integrity, efficiency, and adoption of enterprise-wide AI systems.

> "*Global history knows many cases when large, global corporations and even countries literally slept through a technological breakthrough and were swept off the historical stage overnight*[vi]*.*" — Vladimir Putin

References

[i] The use of scenarios as a support for decision-makers is not new. It is thought to have been the brainchild of Herman Kahn of the Hudson Institute to permit visualization of nuclear war. Pierre Wack, a London based economist with Royal Dutch Shell, is thought to have been first to adapt scenarios for use in business strategy — now in use for over fifty years by a variety of organizations. Led by London based Pierre Wack (Author of HBR articles: Scenarios: Uncharted Waters Ahead and Scenarios: Shooting the Rapids), Arie DeGeus (The Living Company), and Kees Van der heyden (Scenarios: The Art of Strategic Conversation), some of their research has not been made public even today. It was popularized in the US by Global Business Networks' Peter Schwartz in his book *The Art of the Long View*.

Though scenario planning was adopted in some parts of the Department of Defense, it was not widely brought into practice, and Pierre Wack is still considered an "unconventional French oil executive", but the outcome for Royal Dutch Shell dealing with the oil shocks of the 1970s was an exceptional success.

[ii] Aristotle 980a Metaphysics, Translated by W.E. Ross

[iii] Although the names have been changed, this scenario is based on actual people, events, and organizations.

[iv] HumCat was a 2017 honoree of Innovation New Mexico by the Albuquerque Business Journal

[v] Metamorphic Transformation with Enterprisewide AI, by Mark Montgomery, presented at ExperienceITNM on 9/13/2019, IEEE Rising Stars on 1/04/2020, and University of South Dakota on 11/19/2020.

[vi] Artificial intelligence is not about hype, it will not 'fade away' over time. — Vladimir Putin