Evolution VS. Extinction

What cybersecurity professionals could learn from nature to build a more resilient career

BY CATHERINE KOZAK

MINUSCULE FRUIT FLIES have been doing their thing for 40 million years, somehow managing for millennia in southern Africa on a diet of marula fruit. After a fateful meetup about 10,000 years ago with multiple-fruit-loving humans, the insect promptly started evolving to the non-fussy generalist we know today.

"Their offspring then colonized the world," Marcus Stensmyr, senior lecturer at Lund University in Sweden, says in a 2018 news statement about his research. "It's actually quite awesome."

Although the humble fruit fly may not be awe-inspiring beyond the science laboratory, its very existence offers a valuable lesson on how to build a resilient cybersecurity career: Diversify. Seize opportunities. Adapt. Evolve. Have a back-up plan.

Faced with the multiple shocks of 2019-2020—the political divide, the pandemic, nations' reckonings with race and gender, the economic shutdown, not to mention a series of raging wildfires and vicious storms—it would behoove cybersecurity professionals to remember that we're all subject to the same internal and external environmental forces. Unless you're a crocodile, staying put and doing the same thing when under duress is rarely rewarded by nature.

“Arguably, evolvability is the best way to be resilient because even broad or highly dependable niches will be threatened eventually.”

—JASON BERTRAM, THEORETICAL BIOLOGY FELLOW AT THE ENVIRONMENTAL RESILIENCE INSTITUTE AT INDIANA UNIVERSITY

There’s a reason for the fruit fly’s endurance. For example, the *Drosophila melanogaster*, with a brain the size of a poppy seed, has evolved into a winter and summer version of itself. The tiny fruit flies even have complex courtship rituals that rival species one thousand times their size.

Jason Bertram, Theoretical Biology Fellow at the Environmental Resilience Institute at Indiana University, has spent considerable time constructing models that illustrate how complex biological systems interact with and respond to their environments—and change them.

Of course, he has studied generations of fruit flies, a species that has contributed immeasurably to understanding cellular mechanisms and genetic variation in evolution and which go through their entire lifecycle in a matter of weeks.

“For example, evolutionary biologists have set up fruit fly populations in a wind tunnel,” he says in an email interview, “and they have evolved to fly more than 10 times faster than even the fastest fly we would measure in a natural population without new mutations contributing.”

Bertram, who himself has gone through multiple evolutions with an undergraduate degree in mathematics from the University of Cape Town, a master’s degree in physics at Australian National University (ANU) and a doctorate in biology from ANU, became fascinated with collective behavior while studying the physics of plasma, a population of charged particles.

Switching to ecology, his focus was broadened to looking at how organisms adapt to, and evolve as a result of, environmental change—how quickly and by what means? Would those adaptations, in turn, shift the surrounding ecosystem? In addition to his primary focus on adaptive evolution and rapid adaptation, Bertram is now studying how human-caused climate change differs from any previous environmental change Earth has experienced.

Despite his interest in collective behavior, Bertram was wary about making conclusions about the “balance” of life. But he did agree a career analogy could be made.

“The history of life on Earth is one of tremendous change, even when we zoom in on the recent lives of organisms that are alive today,” he says, “Biologists often use the term ‘niche’ to describe an organism’s place in an ecosystem.” And taking a leap into the business world, he noted the coincidence of “niche” being used to describe how we make our living.

“Ecologists generally view resilience in terms of having a broad niche: i.e., you are flexible in how you make a living,” he continued, “and can thus survive in a wide variety of different environments, ensuring that changes to one environment don’t eliminate you.”

Being “evolvable” is having the ability to change a niche when the environment changes, he says. An outcome known as “evolutionary suicide” can result, however, when selection is focused on short-term results to the detriment of long-term gain.

ENVIRONMENTAL IMPACTS

Evolution—the science of which is still evolving—is geared toward immediate outcomes, in that selection rewards attributes that favor survival and reproduction in those conditions, Bertram explains. But there is evidence that past evolution produces attributes that are essentially shelved until they become useful again, if and when a similar environment returns.

“Arguably, evolvability is the best way to be resilient,” he says, “because even broad or highly dependable niches will be threatened eventually.”

Stretching the metaphor, clearly the cybersecurity industry, though still evolving, has not yet gone beyond the Neanderthal stage. Cyber professionals know how to use tools and they’re great at hunting, but the rules and culture are hardly set in stone, so to speak.

With much of the world now connected digitally, cyberattacks have

"Just in general, there's great pressure to specialize in one's career, and that can be very good until there's a major shift, and what you're specialized in may become obsolete."

—ALICE HILL, SENIOR FELLOW FOR THE COUNCIL OF FOREIGN RELATIONS

become an increasing problem, costing global economies an estimated $400 billion annually, according to the CyBOK website.

Funded by the National Cyber Security Programme and led by the University of Bristol, CyBOK—which stands for cybersecurity Body of Knowledge—was launched in 2018 as an international effort to unify professional standards and training in fast-growing technology industries.

Mature scientific disciplines such as biology and chemistry, it states, have established bases of knowledge and clear steps to teaching the skills. "However, there is a long-recognized skills gap within the cybersecurity sector," the CyBOK site says, "an issue that experts agree is compounded by a fragmented and incoherent foundational knowledge for this relatively immature field."

To compound the challenges in cybersecurity, there is still a critical shortage of qualified cybersecurity professionals: about 4 million more trained cybersecurity professionals are needed today, according to various industry studies, including (ISC)²'s latest Cybersecurity Workforce Study.

On a broad level, one of the big problems facing the industry is the discrepancy in salaries for government and private sector jobs, says Alice Hill, Senior Fellow for the Council of Foreign Relations. As a result, federal government agencies often struggle to find and keep qualified staff.

"Now the government is maintaining a lot of systems, some of them deeply out of date … with some substantial vulnerabilities," she says. "Yes, we should have the very best helping protect against that, protecting our nation from attacks."

But as issues with managing health data and distribution of unemployment insurance payments during the pandemic have shown, problems with technology in government agencies is systemic, and budgets are only going to get worse for a while.

"I remember going to a Black Hat conference and meeting with a bunch of hackers, talking about the need for help for the federal government," Hill recalls, "and one of them told me, 'You can try to sell us on serving our country, but your salaries just don't match what we can make elsewhere, so you're going to have a hard time finding anyone.' And that turned out to be [true]—it was a very difficult task."

BOUNCING BACK

Hill, who in a previous life served as a special assistant to President Barack Obama and Senior Director for Resilience Policy on the National Security Council, as well as advisor on policy related to creation of the U.S. Department of Homeland Security's cybersecurity workforce, says that she is now focused more on climate change than cyber issues. But, she sees important similarities. Both are vast, interconnected systems that are directly linked to national security.

And there has yet to be sufficient political will to create policy measures to comprehensively address risks from climate change—sea level rise, species extinction, intensified storms, increased drought and wildfires—and the cyber vulnerability of infrastructure, including energy, weather satellites and communication systems and economic systems, to public and private data breaches and attacks.

"With both cyber and climate change, we have huge risks that are growing exponentially," Hill says. "And it's difficult for humans to stay ahead of them. So, what we're seeing is that we're playing catch-up. And that increases the role of vulnerability.

"I think the goals are the same: that we be able to prepare for and recover from, bounce back from, bad events. But similarly, we are unprepared at this stage, I think it would be fair to say. And I believe that both of these threats require a more systematic approach, deeper planning for how we will have a system that allows us to be resilient. We're just in the beginning for both of these threats, I think."

RETURN TO CONTENTS

Even if one company is vigilant in protecting itself from malware, for instance, that won't protect whoever is connected to their systems.

"A failure in one system can spread to another," Hill said, "and that's very similar with climate change. But it's hard to protect yourself entirely. Particularly with cyber, there are bad actors who are trying to actively exploit vulnerabilities."

There should be standards for resilience in both cyber and climate, and expectations that people will meet them, Hill says. Use incentives and employ penalties "to drive better compliance and better practice."

WINTER IS COMING

Again, resilience in navigating a career in a rapidly evolving field can be inspired by survivors in nature. Prepare for winter, and don't depend on one thing to survive.

"Just in general, there's great pressure to specialize in one's career," Hill said. "And that can be very good until there's a major shift, and what you're specialized in may become obsolete."

Her advice for a resilient career is to keep building skills. Look at opportunities that come your way.

"Think about: 'Does this teach me something new? Does it allow me to do things that I haven't been able to do before? Will it stretch me? Does it hone existing skills?' And when you get more yes's than no's, it's a more promising thing to do."

Often, Hill has seen people who, because they're good at their jobs, believe that is good enough. "But I think with the scope of the careers I've observed, circumstances continue to change. And it is people who are most nimble who are the ones that have continued to develop their skills. … You can use (them) to develop your network. So you know people doing different kinds of things. And then you can make switches in your career more easily."

But survival comes down to the environment you are living or working in, and whether you adapt, fly off or starve. Companies, after all, are a kind of ecosystem, except leadership creates the conditions instead of nature.

"The biggest threat is disengaged employees," says Johanna Lyman, Principal Consultant and Practice Leader for Culture and Inclusion at Kadabra SJLC.

Lyman says only about 30% of employees are "truly engaged" with their job, about half float through their days on autopilot, and about 20% are toxic and "poisoning the well for everybody else."

That all adds up to about $500 billion a year in lost revenue for U.S. companies, she says. But if there's one thing a company, and especially its IT department, does not want, it's employees who are sleepwalking or untrustworthy.

"If you've got disengaged employees, do you think they're going to be really careful about the code that they're writing?" Lyman asks. Or, in a toxic situation, the employee "could be actively working against security."

The solution comes from the top, she says. Leadership must foster inclusion and a sense of belonging in the company. Ask employees their opinions. Unite everyone around a mission beyond the bottom line or enriching stockholders.

"If you have a purpose beyond just making money, and if you are actually embodying that purpose, you've got your core values," she says. "Everybody knows what that looks like in action. Everybody knows what the purpose is. And they can see the company working toward it on a regular basis."

Or alternatively, a troubled company or cyber career may make no changes or adaptations. It doesn't evolve.

Instead, it dies off. ■

> "If you've got disengaged employees, do you think they're going to be really careful about the code that they're writing?"
>
> —JOHANNA LYMAN, PRINCIPAL CONSULTANT AND PRACTICE LEADER FOR CULTURE AND INCLUSION, KADABRA SJLC

CATHERINE KOZAK *is a freelance writer specializing in environmental reporting who is a past contributor to* InfoSecurity Professional.