Taking IT Operations From Phoenix to Hydra Dragon

If there is a choice between being a phoenix or a hydra dragon, which option would be better? Both are ancient mythical creatures with supernatural powers. The phoenix is an immortal bird associated with Greek mythology. It is known for its ability to rise from ashes. It burns out and repeatedly rises to its previous magnificent state, gaining new life from the ashes of its predecessor. Conversely, the hydra dragon is a mythical creature associated with Roman mythology—a water monster with a multitude of heads. When one head is cut off, two are regenerated from the fresh wound. The hydra dragon has poisonous blood and breath that makes its scent deadly. But how do these two powerful creatures relate to IT operations?

For decades, the focus of IT operations was on maintaining stability, compliance and maturity by facing—and recovering from—disruptions (e.g., systems outages, equipment failures, natural disasters, cyberattacks). The goal was to be a phoenix in the dynamic and ever-changing world of technology, rising from the ashes and adapting as needed. Operations teams were programmed to be prepared to respond to disruptions and return to normal after disruptions, which is also known as resilience—the capacity to recover quickly from difficulties.

ABDELELAH ALZAGHLOUL | CISA, CRISC, CISM, CGEIT, ITIL 4 MP, ITIL 4 SL

Is an IT advisor with 17 years of experience in IT governance, service delivery and IT transformation programs. He is experienced in the deployment of various IT governance frameworks and standards in the telecommunications sector. He is also a certified trainer in IT governance and the service management fields.

Resilience was tested in 2020 when the world was faced with the onset of the COVID-19 pandemic, which was unprecedented in modern history. The pandemic's devastating impact is still being felt across the world, and it has led IT organizations to recognize that being resilient may not be enough. The need is not only to recover from disruptions and return to normal, but to actually become stronger than before. In other words, IT organizations now need to act as a hydra dragon that regenerates new heads if one is cut off by disruption. This state is defined as antifragility, or gaining from disorder.[1]

Moving from resilience to antifragility, or from a phoenix to a hydra dragon, requires IT organizations to leverage continual experimentation as a means to explore, inspect and adopt technology advancements and anticipate future sources of disruptions. Many organizations have followed this path of continual experimentation and achieved success, including:

- **Netflix and its Simian Army**—Chaos engineering as a tool to induce disruptions to production environments[2]
- **Google's site reliability engineering (SRE)**—A mindset and a set of practices, metrics and prescriptive ways to ensure systems' reliability through treating operations as a software problem[3]
- **Spotify's Agile model**—A people-driven, autonomous approach for scaling Agile that emphasizes the importance of culture and networks[4]

None of these stories emerged overnight. Each of these enterprises has undergone considerable experimentation, failure and readjustment to reach the degree of success such that other organizations

begin to mirror their practices. What IT organizations should seek to mimic is the institutionalization of a continual experimentation process to be built into an organization's DNA, similar to other IT service management (ITSM) processes (e.g., change enablement, incident management). This new process, which is currently taking place on an *ad hoc* or accidental basis in some organizations, has characteristics that require a shift in mindsets and employee culture (e.g., continuous trendspotting, continuous failure, continuous experimentation) (**figure 1**).

Continuous Failure

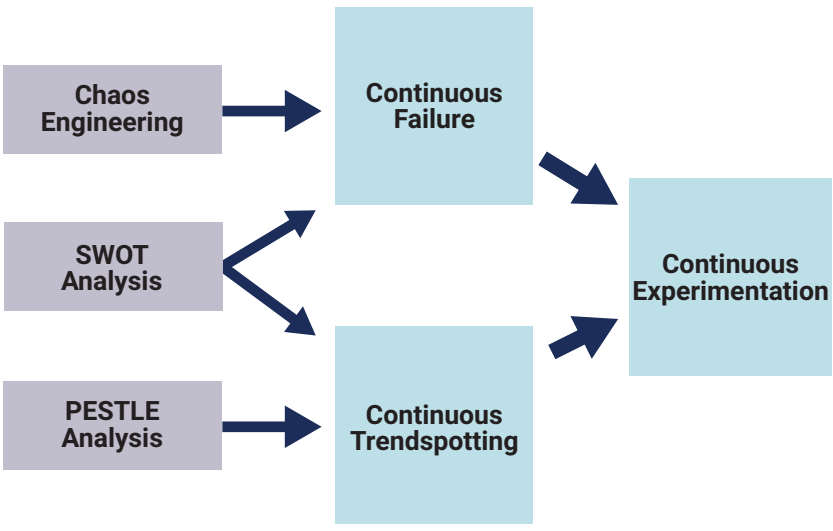
Continuous failure is a term often used to refer to exposing IT operations to calculated and intentional disruptions with the sole purpose of learning and improving from and after failure. The word "continuous" is often used in DevOps discussions and refers to activities that are automated and frequently performed. In 2011, Netflix introduced Chaos Monkey, a tool that intentionally disables production servers to test how remaining systems respond to the outage. Since then, more tools were added to build its Simian Army, a suite of automated tools engineered to stress test Netflix's infrastructure and proactively identify weaknesses so that they can be resolved. The Army is comprised of additional tools such as Chaos Gorilla and Chaos Kong that intentionally induce failure through means such as random interruption or slowness so that issues can be identified and fixed before they surface and impact customers.[5]

The broader concept is called chaos engineering, which is the discipline of experimenting on a system to build confidence in its capability to withstand turbulent conditions in production.[6] There are various chaos engineering tactics that can be used, including:

- **Continuous resilience**—Inducing calculated failure to components, systems and services in an attempt to enhance overall continuity plans. In this case, "calculated" means risk has been assessed and random chaos only occurs when managers, operators and developers are present to address any urgent situation that might be caused inadvertently.
- **Continuous penetration**—Continually exposing IT systems and processes to simulated cyberattacks or even baiting adversaries to perform specific tasks by providing easy access to nonproduction environments and intentionally compromised systems, allowing attackers to exploit vulnerabilities so security teams can study them to improve the overall security posture. Many techniques can be used to achieve such objectives, including:
  - **Ethical hacking**—Ethical hackers, also known as white hat hackers, do not intend to harm the system or organization; they do so, officially, to penetrate and locate vulnerabilities and provide solutions to fix them and ensure safety.[7] Organizations legally engage ethical security engineers to identify vulnerabilities and discover breaches or threats in infrastructure, networks, data and applications, enabling the organization to collect and analyze the information to figure out ways to strengthen security controls and policies.
  - **Honeypots**—In the world of espionage, the term honeypots is used to describe how romantic relationships are strategically used to steal secret information. In cybersecurity, honeypots work in a similar way by attracting attackers to a virtual

> "What IT organizations should seek to mimic is the institutionalization of a continual experimentation process to be built into an organization's DNA."

FIGURE 1
Continuous Failure, Experimentation and Trendspotting



trap that consists of intentionally compromised systems, software, servers or networks to understand attackers' behaviors and patterns. Although honeypots are not used as often in IT operations, they are still an option. Different types of honeypots can be used to identify different types of threats, for example:

- **Spider honeypot**—Intended to trap web crawlers, malicious bots or ad network crawlers
- **Decoy database**—Intended to trap attackers targeting system architecture or using Structured Query Language (SQL) injection
- **Honeynets**—Intended to trap network attackers. Any outbound activity on a honeynet is likely evidence that the network is compromised.

Continuous failure aims at anticipating disruptions before they occur, thus giving individuals and organizations the opportunity to be alert, prepared and equipped with knowledge and experience gained from responding to different scenarios on an ongoing basis.

"A good safety culture is generative in nature; it cannot be enforced, but it can be promoted by the commitment of senior management."

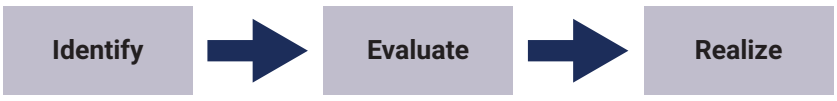
Continuous Trendspotting

Analyzing future trends across technical and nontechnical domains is essential for organizations willing to introduce and leverage innovation. Innovative approaches and technologies, especially when explored during the early stages of development, offer organizations more potential to create value and improve performance before competitors. Innovation can also help organizations become more resilient. Continuous trendspotting and foresight is an approach through which organizations can evaluate future trends and how they impact their operations. Transformative or disruptive trends are normal results of the volatile, uncertain, complex and ambiguous (VUCA) world of today. Organizations often inadvertently adopt *ad hoc* or accidental approaches to innovation, either by responding to a disruption or focusing on short-term observed trends. Institutionalizing trendspotting means moving to a more purposeful approach to innovation, where both short- and long-term trends are explored, evaluated and realized. A simple process to structure innovation may consist of three stages (**figure 2**):

1. **Identify**—Analyzing and exploring future trends across domains to generate, prioritize and select potential ideas for further examination based on cost-benefit analysis. Political, economic, sociological, technological, legal and environmental (PESTLE) analysis can be used to identify key drivers or potential opportunities outside the organization.
2. **Evaluate**—Defining and testing a hypothesis for selected ideas and estimating the potential impact on business in terms of value and risk. Proof of concepts can be leveraged to simulate such impact.
3. **Realize**—Scaling up the evaluated idea from the innovation garage or laboratory to production, where benefits can be realized and measured

Trendspotting requires a balanced approach since a mistake that is often made in IT is focusing on technology while ignoring other trends that also have significant impact on organizations, such as changes in business models, social patterns and emerging work practices.

FIGURE 2
Continuous Trendspotting



Continuous Experimentation

The success of both continuous failure and continuous trendspotting relies on the adoption of a culture that fosters and embraces continual experimentation. Such safe-to-fail cultures provide IT professionals with physiological safety and a blameless environment where they can talk and act without fear of reprisals. A good safety culture is generative in nature; it cannot be enforced, but it can be promoted by the commitment of senior management providing their teams with the tools, resources and behavioral patterns required to foster such culture. A servant leadership style is an example of how management can serve or facilitate rather than manage. A servant leader would exhibit characteristics such as:

- Working toward a vision
- Leading with questions
- Demonstrating patience
- Stimulating teams intellectually
- Developing teams and individuals

An important role for servant leaders is to provide their teams with the tools required to practice continuous trendspotting and continuous failure, including:

- **Education and learning opportunities**—Provide teams with access to knowledge sources that include:
  - Subscriptions to global technology magazines, journals and research institutes
  - Subscriptions to self-paced and online training providers
  - Promotion of communities of practice (i.e., organized groups of people who have a common interest in a specific technical or business domain where people can collaborate and expand their knowledge)
  - Promotion of individuals sharing their acquired knowledge by publishing articles and newsletters in addition to conducting knowledge-sharing sessions
- **Innovation centers (also known as hubs or garages)**—Offer research and development (R&D) platforms where teams and individuals can practice and experiment with new ideas, technologies and ways of working. Employees from different units and with varying experience levels come together and work hand in hand away from day-to-day tasks to try new things and innovate. Institutionalizing innovation has become a major enabler for organizations to survive in this constantly changing world, and many global firms have launched innovation accelerators to support organizations in adopting new ideas and realizing value at the fastest and most efficient rate. IBM introduced IBM Garage as a model for accelerating digital transformation that helps organizations generate innovative ideas and creating business value.[8]

  A key tool to encourage individuals to spend more time in innovation labs is arranging technology competitions such as hackathons or codefests, where members from different units establish teams and collaborate to develop new products or try new ideas.

"Many global firms have launched innovation accelerators to support organizations in adopting new ideas and realizing value at the fastest and most efficient rate."

Continuous experimentation is vital to promoting a continuous learning culture where employees are given the opportunity to learn while they work and continually acquire new skills and knowledge.

Conclusion

Resilient (phoenix) systems, organizations and people are able to easily return to a normal, healthy state after experiencing a disruption by using defenses and experiences learned from past incidents. However, today's VUCA world requires organizations to move from the state of resilience to antifragility (hydra dragon) by taking further steps such as continuous failure, trendspotting and experimentation, so that organizations no longer wait for disruptions to occur and instead seek out disorder and anticipate what could be the next major disruption to generate new heads and become a stronger hydra dragon.

Endnotes

1 Nassim, T.; *Antifragile*, Random House, USA, 2012
2 Izrailevsky, Y.; A. Tseitlin; "The Netflix Simian Army," The Netflix Tech Blog, July 2019, *https://netflixtechblog.com/the-netflix-simian-army-16e57fbab116*
3 Franko, G.; "Do You Have an SRE Team Yet? How to Start and Assess Your Journey," Google Cloud, January 2019, *https://cloud.google.com/blog/products/devops-sre/how-to-start-and-assess-your-sre-journey*
4 Cruth, M.; "Discover the Spotify Model," Atlassian Agile Coach, *https://www.atlassian.com/agile/agile-at-scale/spotify*
5 *Op cit* Izrailevsky
6 Principles of Chaos; "Principles of Chaos Engineering," March 2019, *https://principlesofchaos.org/*
7 EC-Council, "What Is Ethical Hacking?" *https://www.eccouncil.org/ethical-hacking/?_ga=2.224407704.381612571.1630142171-57869435.1630142171*
8 IBM, IBM Garage, *https://www.ibm.com/garage*

JOIN THE DISCUSSION

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*