Deloitte.
CIO Insights and Analysis from Deloitte

The Nature Lover's Guide to Cyber Security

Biomimicry is catching on in the cyber security field as engineers take inspiration from nature to develop improved technologies for protecting data and thwarting cyber crime.

Imitation is readily acknowledged as the sincerest form of flattery—except among innovation purists. No one wants to be accused of copying others' ideas, right? Today, though, being a "copycat" is *de rigueur* if the source material comes from nature.

Biomimetics, or, as it's popularly known, "biomimicry," is a fast-growing field in which researchers explore how animals, plants, humans, and even micro-organisms perform certain tasks, and then appropriate those biological designs to endow technologies with the same capabilities. Rather than re-invent the wheel, developers of medical treatments, agricultural products, military equipment, apparel, computers, and more are making improvements based on what already exists in the natural world.

For example, the soles of geckos' feet recently helped a Stanford University researcher develop an adhesive that allows robots to climb buildings and other smooth surfaces. Elephants' trunks led to the development of a new type of robotic arm that is said to be powerfully strong and flexible—able to expand and contract by deflating sacs between the "vertebrae." The fins of humpback whales inspired improvements to fan and turbine blades that reduce drag, increase speed, and improve energy efficiency. (For more examples, read "14 Smart Inventions Inspired by Nature: Biomimicry.")

Now biomimicry is catching on in the cyber security field, as engineers seek to protect data and thwart cyber crime using defense mechanisms found in nature.

Bornean moths, for instance, protect themselves from birds by creating leaf tents. Using a similar principle, "data masking" shields sensitive personal information from unauthorized viewers by replacing it with phony data.

The chameleon protects itself from predators by changing colors to blend in with its surroundings, rendering itself nearly invisible. In cyber security, steganography disguises sensitive data to make it look like something else: a picture of a flower, perhaps, or a music file.

Ants and bees work collaboratively to accomplish such tasks as building, defending, and repairing their nests and hives. Similarly, cyber security researchers are applying "swarm intelligence." In one project, "digital ants" continually monitor systems for anomalies such as malware, and drop "markers" where unusual activity occurs, similar to the pheromonal markers ants place along paths to food. When the markers at a given location exceed a certain threshold, an alarm is triggered.

The body's immune system is another popular source of inspiration for cyber security design. Immunity-based systems are always on, alert to anything out of the ordinary, and able to promptly kick into attack and repair mode. And they're adaptive, "remembering" the intruder for increasingly efficient and effective defenses. Some data security systems operate similarly, knowing the "baseline" for normal behaviors, such as the keystroke speeds and patterns of specific users in order to detect potentially unauthorized users.

What other functions might cyber security designers borrow from nature?

- Capsids—the strong, stable containers housing viral DNA—assemble themselves automatically. Could we design digital security that does the same, with multiple organizations on a network responding automatically and in sync to defend against an attack?

- After leaving their chicks to find food, returning penguins can identify their offspring even in a crowd. How might we program our security systems to identify users who don't belong, such as data thieves or "advanced persistent threats" that lurk on our networks long before we discover them?

- Salmon hurl themselves upstream to spawn in the place where they were hatched. They then die, their life's work completed. What if data, after serving its purpose, "expired" and disappeared, no longer vulnerable to theft?

It seems paradoxical, this borrowing from the natural world to safeguard a virtual one. But humans have engaged in biomimicry for eons, starting, perhaps, with wearing animal hides for warmth. Now, as then, we may find some of the best solutions to our problems on nature's path.

—by JR Reagan, global chief information security officer, Deloitte Touche Tohmatsu Limited (DTTL)

January 4, 2016, 12:01 am

Questions? Write to deloitteeditor

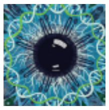
Follow us on Twitter @Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see http://www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting. This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication. Copyright © 2016 Deloitte Global Services Limited.

Search CIO Journal SEARCH

Related Deloitte Insights

- **IoT Opens New Door for DDoS Attacks**
  Insecure internet of things devices could contribute to more damaging and more frequent distributed denial-of-service attacks this year, according to Deloitte Global, thanks in part to the fact that their user IDs and passwords are sometimes hardcoded. In the wrong hands, those credentials can be used as part of a botnet to launch a DDoS attack.



- **Moving Beyond Passwords**
  Most online interactions today begin with a transaction that's both a poor user experience and one of the weakest links for corporate security: the password-protected login. Fortunately, new technologies now coming to the fore promise to enable a world with both security and convenience—and no passwords.

- **DDoS Attacks Enter the Terabit Era**
  Distributed denial-of-service attacks are not a new problem in 2017, but three underlying trends could make them more severe, Deloitte Global predicts. Organizations at risk can take several steps to help mitigate the threat, including designing deceptive approaches that establish a false reality for attackers or disperse adversarial traffic.

Editors Choice

- **M&A Shines Spotlight on CIOs, Tech**
  M&A and divestures may be on the increase in 2017. Because technology is both a top driver of M&A and an important factor in achieving a successful M&A transaction, CIOs have a valuable role to play throughout all stages of the deal process.

- **Tech Trends 2017: An Overview**
  CIOs who can harness the possibilities of emerging technology trends likely to disrupt businesses in the next 18 to 24 months—among them dark analytics, machine intelligence, mixed reality, and everything-as-a-service—will be better positioned to help shape the future of the kinetic enterprise.

- **Rising to and Beyond CIO**
  The CIO role is more of a journey than a destination, according to former Mars CIO Steve Larrabee, who also served as president of Mars Global Services. Larrabee's top tip for aspiring CIOs: Don't wait until you have the title to start thinking like a CIO and imagining opportunities to bring value beyond it.

About Deloitte Insights

Deloitte Insights for CIOs couples broad business insights with deep technical knowledge to help executives drive business and technology strategy, support business transformation, and enhance growth and productivity. Through fact-based research, technology perspectives and analyses, case studies and more, Deloitte Insights for CIOs informs the essential conversations in global, technology-led organizations. **Learn more**