HATCH™

Innovation born in San Diego ● Vol. 2, No. 2

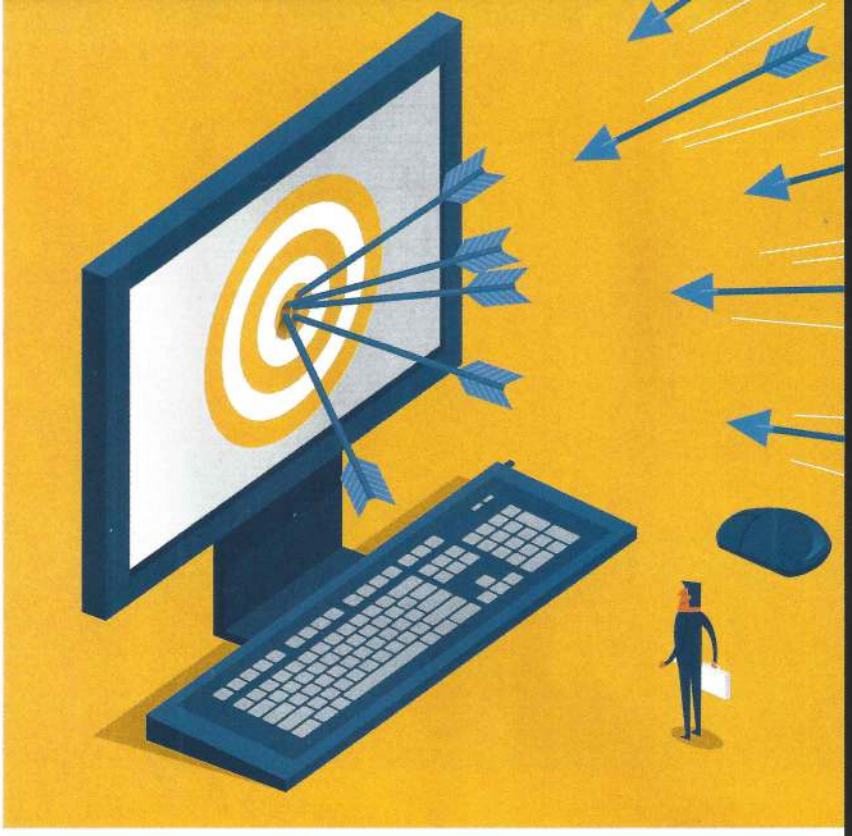
ANIMAL FARM

A new frontier in farming begins with bacteria from a San Diego lab.

opinion

Why you need a CISO

If you don't already have one, you're behind the times and possibly at risk



We can't escape the daily headlines detailing massive data breaches. A billion compromised user accounts at Yahoo and a state-sponsored hack intended to sway our presidential election results demonstrate that cybersecurity has rapidly become a global crisis. For private companies, a serious amount of risk hangs in the balance: Cybersecurity Ventures predicts that global annual cybercrime costs will grow from $3 trillion in 2015 to $6 trillion by 2021.

As someone who helps companies navigate the communications challenges presented by data breaches and security threats, I am consistently surprised that so many executives are still unprepared for these circumstances. The likelihood of a data breach or hack has reached a status of "when," not "if." Yet at many companies, the proverbial "IT guy" often sits in a back room, used only as a resource for minor technology issues, like when an employee says their computer isn't working. The IT team often isn't privy to C-suite business decisions, and therein lies the problem.

Enter the chief information security officer (CISO). A CISO is a top-level executive role, and is included in boardroom discussions to ensure that the executive management team understands the company's cybersecurity risks and factors them into business decisions. Security should augment and facilitate the flow of business, and upper management must help remove obstructions and impediments that compromise security of the company's most critical assets: corporate and customer data.

"The idea that a hacker is a lone wolf in a basement is dangerously outdated: Most successful cybercriminals are recruited and trained by established organized crime groups funded by governments."

Cybercriminals have evolved faster than most security systems. Their ability to conduct network surveillance and launch distributed denial-of-service (DDoS) and phishing attacks is designed to either monetize stolen data, such as credit card numbers, or expose sensitive company information. The idea that a hacker is a lone wolf in a basement is dangerously outdated: Most successful cybercriminals are recruited and trained by established organized crime groups funded by governments to take advantage of social media and email communications. A CISO would not only analyze, formulate, and mitigate security risks, but also forge partnerships with supporting business operations teams, community cybersecurity organizations, and federal and local law enforcement to stay at the forefront of security issues.

Most boards and executives are not typically fluent in matters of information technology. Who better to educate the board on cybersecurity and regulatory issues than your CISO? Knowing that the board has a fiduciary obligation to protect shareholder value, the role becomes a win-win scenario. After all, the most security-aware a company will ever be is immediately after a breach. Don't wait until it's too late!

→ Kevin Dinino is president of KCD PR and a board member for the San Diego Cyber Center of Excellence.

SHOUT-OUT TO SD CISOS

Several local companies have a chief information security officer in their C-Suite—and so does city hall!

Frank Bunton
MedImpact Healthcare

Tina Lovoy
Welk Resorts

Jason Callahan
Illumina

Terrence Weekes
DJO Global

Gary Hayslip
City of San Diego

Kris Virtue
Qualcomm

Powell Hamilton
Scripps Health

Todd Friedman
ResMed

Kim Van Nostern
Charlotte Russe

Jason Harkins
Sony Network Entertainment