Deloitte.

THE RIPPLE EFFECT

Stories of purpose and lasting impact

Finding more bang for the cyber buck

Cyberthreats increasing; costs rising. Cyber capabilities need to be maintained; spending needs to be reduced. What to do?

ENTER **CYBER COST OPTIMIZATION,** A **STRATEGIC APPROACH** TO CYBER SPEND.

THE SITUATION

In the past five years, the average price of a humble grocery store chicken egg has increased 160%. There are a bunch of reasons for this, but that egg is a good example of how prices have been rising nearly everywhere.

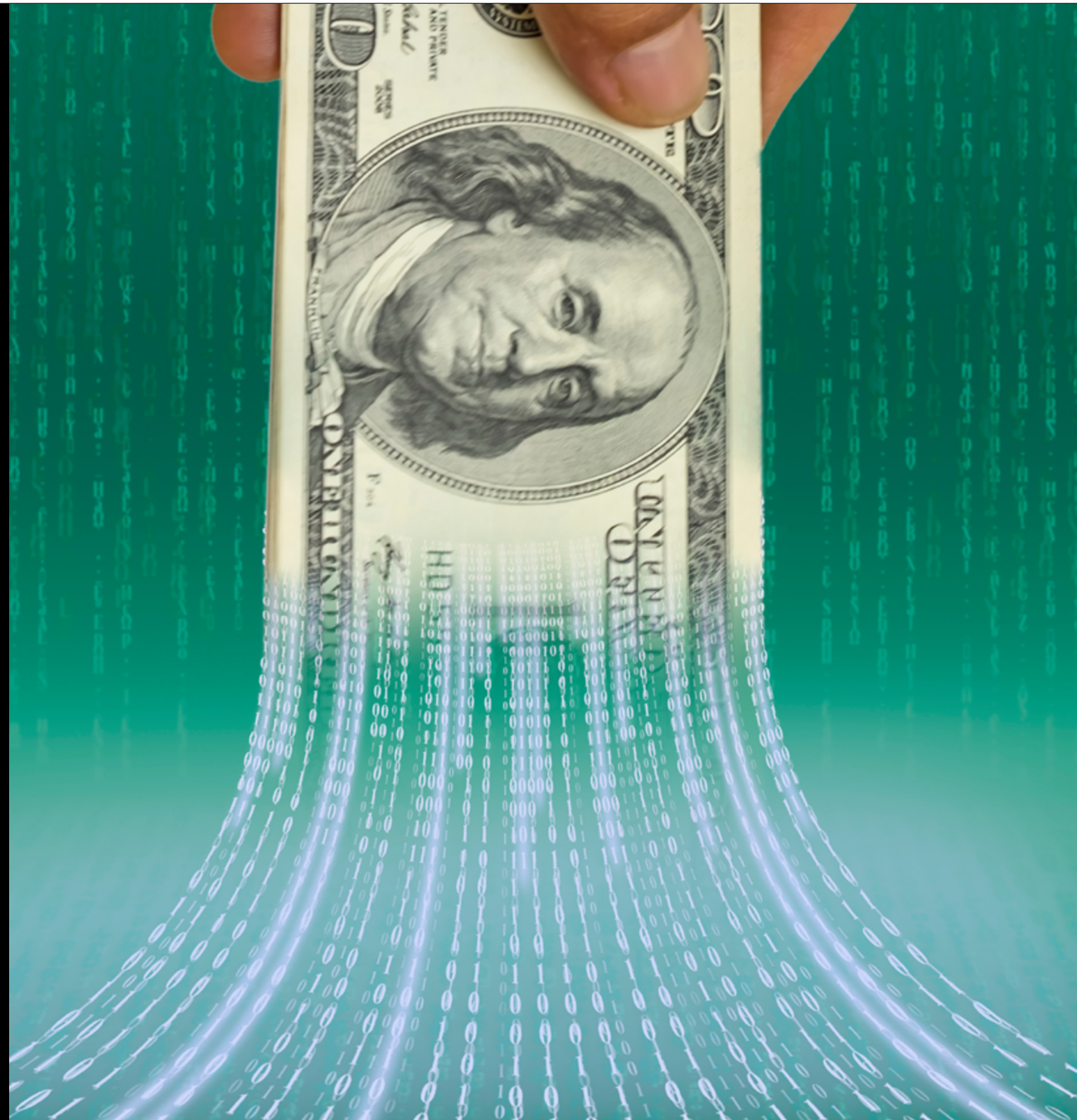
Everywhere, including the cybersecurity arena, where costs are also soaring—for a bunch of different reasons. Reasons like widespread digital transformation—great for businesses and customers; also great for bad actors who now have more opportunities to exploit (thus requiring more resources to manage and mitigate). Reasons like increased cyber regulatory requirements. The European Union's Cyber Resiliency Act and several provisions of the Consolidated Appropriations Act, 2023 in the United States are just two examples of the added compliance responsibilities organizations must contend with (and thus pay to manage). Then there's the severe shortage of skilled cybersecurity professionals, which makes cyber talent acquisition and retention a major (and costly) challenge.

Taken together, these forces are putting chief information security officers (CISOs) in a pickle: how can they, in such an inflationary environment, continue to secure and protect their organizations from cyberthreats…in a fiscally efficient way?

One CISO in particular—an executive at a global life sciences and health care company—found themselves in just such a pickle, and then some. Not only were they contending with the garden-variety challenges their peers were, but also supply chain issues and recessionary fears had company leaders looking closely at spending overall, cybersecurity budget included. Belts were going to be tightened. The message was clear, if unspoken: Either come up with a more streamlined cyber budget that doesn't cut corners on cyber protection or have one handed down.

So threats were increasing, costs were rising, cyber capabilities needed to be maintained, yet cyber spending needed to be incrementally increased… but in a way that could be more directly tied to risk reduction and value to the business. This left the CISO with only one option: do more with, effectively, the same resources. But how?

For an assist, they called professionals with Deloitte's Cyber Risk Services. The task at hand: cost optimization.



THE SOLVE

Cost optimization is *not* just about saving on costs. Experience had shown the Deloitte team that the most effective way to enhance the company's cybersecurity efforts (while reviewing costs) would be to go to school on how the cyber department managed four domains: workforce, vendors, technology, and the stuff that knit it all together—operations.

The organizing function for this analysis: a proprietary cost optimization framework that includes understanding current spend, defining different strategies to manage cost, and providing insights into the environment with an eye to developing more efficient processes.

This last bit involved getting a sense of how the company stacked up to its competition. Thanks in part to Deloitte's ability to apply its full breadth of thinking, experience, and technology, the team could create a custom cyber industry comparison based on the company's direct competitors.

What was cyber spend as a percentage of revenue? How were workforces structured? (How many employees? How many contractors? How many third-party security service providers? Where in the world did all these resources sit?) This comparison helped the company both confirm its spending and understand whether it was commensurate with its peers. It also served as a litmus test for understanding whether the company was spending more or less in specific areas compared to competitors. (And in cases where there was a variance with its peers, it raised the question: Why?)

Finally, the Deloitte team convened a Cyber Cost Optimization Lab—an immersive session for company stakeholders to work through the data collected in the four domains (workforce, vendors, technology, and operations); workshop options and scenarios; and ultimately land a business case outlining the cost savings and optimization benefits identified.

As the picture started taking shape, one of the framework's cost optimization levers in particular stood out: the company's talent footprint. The data showed that a significant amount of real cost savings could be realized by revisiting the company's workforce location strategy. Then, there was a related opportunity to explore—as a global concern, the company followed a common financial strategy of locating offices in a number of countries. If it applied this same strategy to its cyber workforce and shifted some its in-house roles to countries with a lower cost structure, then it could reduce expenditures even more, even as it benefited from an expanded talent pool.

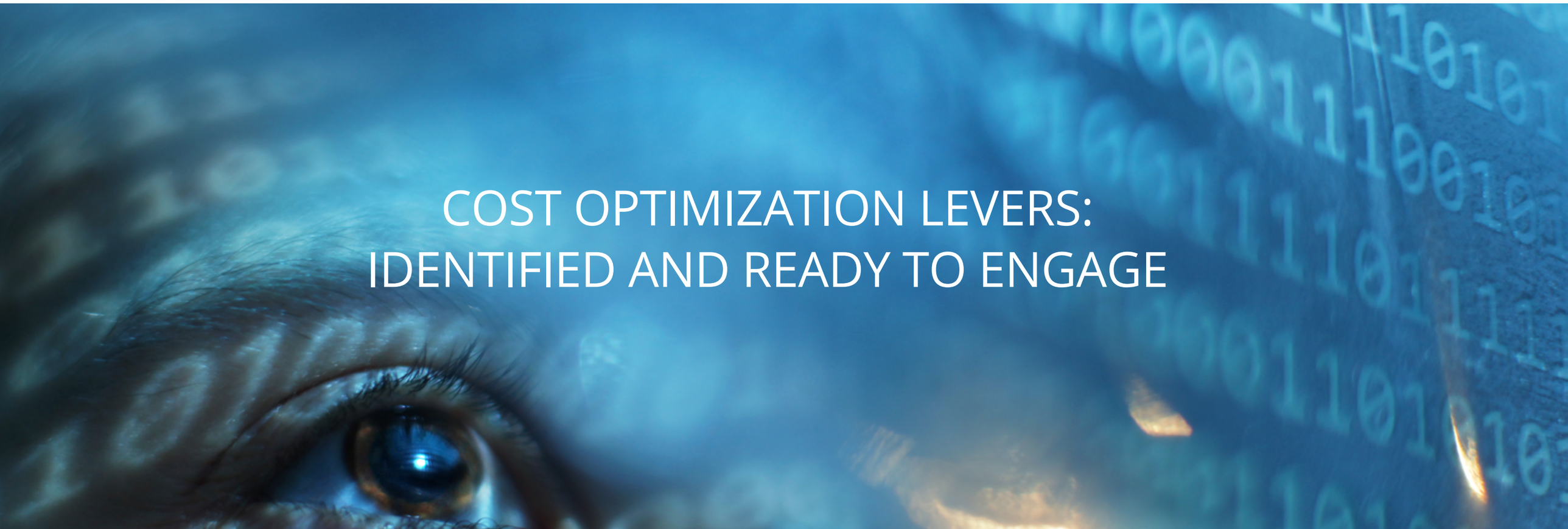
A final consideration centered on the intersection of workforce, technology, and operations: applying new forms of automation and artificial intelligence (AI) to cyber tasks. By so doing, the company could potentially both lower costs and improve cyber readiness as lower-skilled, lower-value activities were shifted to machines, freeing up cyber practitioners for higher-skilled, more rewarding activities.

INDUSTRY COMPARISONS CONFIRM SPEND AND ARE LITMUS TESTS FOR RESOURCE ALLOCATION.

THE IMPACT

By the close of the cyber cost optimization engagement, the CISO had a plan that could both save costs and maintain—even improve—the value of the company's cybersecurity activities while setting a strong foundation for future initiatives (with the distinction of being the first leader in the company's overall technology organization to deliver a roadmap to both optimization and value).

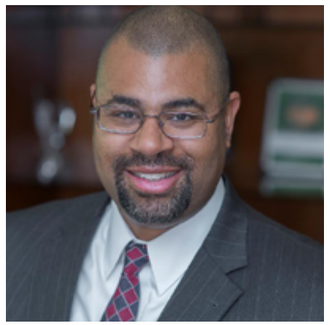
Internal discussions continue about the implications of moving workforce roles—decisions to be carefully investigated and planned, with an eye toward finding the right balance between in-house, onshore, offshore, and external resources to both achieve cost optimization and maintain a mature and stable cybersecurity program.



LET'S CONNECT.

Do these challenges sound familiar?

SUNNY AZIZ
Principal
Deloitte & Touche LLP
saziz@deloitte.com
+1 713 982 2877



RUSSELL JONES
Partner
Deloitte & Touche LLP
rujones@deloitte.com
+1 415 783 5054

SUBHRANSHU PATNAIK
Managing Director
Deloitte & Touche LLP
subhrpatnaik@deloitte.com
+1 470 434 3271

MAINAK SHOME
Senior Manager
Deloitte & Touche LLP
mshome@deloitte.com
+1 470 434 5181

Deloitte.

About this publication

This publication contains general information only and Deloitte is not, 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 business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.