Cybersecurity: How do you rise above the waves of a perfect storm? (PART 1)

ISAAC SARPONG: Isaac is the Partner in charge of Tax Services. He has over 26 years' experience in the provision of multi-faceted advice to both local and international clients in taxation, accountancy, audit & assurance, and corporate law, among others. Isaac is a Chartered Accountant, a Chartered Tax Practitioner and a Lawyer.

EY
Building a better working world

The EY Global Information Security Survey 2021 finds CISOs and security leaders battling against a new wave of threats unleashed by COVID-19.

In brief:

- Cybersecurity is under pressure: 81% of execs say that COVID-19 forced organizations to bypass cybersecurity processes.
- Three challenges stand out: insufficient budgets, regulation complexity, and strained relationships with the business.
- If CISOs can readdress shortcomings with a security by design approach, they will become enablers of growth in the rebound era.

The EY Global Information Security Survey 2021 (GISS) illustrates the devastating and disproportionate impact that the COVID-19 crisis has had on a function that is striving to position itself as an enabler of growth and a strategic partner to the business.

Through a global survey of more than 1,000 senior cybersecurity leaders, we find CISOs and security leaders grappling with inadequate budgets, struggling with regulatory fragmentation, and failing to find common ground with the functions that need them the most.

Indeed, the upheaval of the global pandemic has created a perfect storm of conditions in which threat agents can act. Since the 2020 GISS report, there has been a significant rise in the number of disruptive and sophisticated attacks, many of which could have been avoided had companies embedded security by design throughout the business.

The CISO's relationship with the business is also under more stress than before, and the fallout is greater exposure to cyber risk. On top of that, budget restrictions mean CISOs are struggling to bridge the gap between need and funding.

The situation is likely to get worse before it gets better. Organizations want to invest in technology and innovation for the post-COVID-19 era, and they need to ensure resilience for the next major disruption, but many have yet to address the deferred risks and potential vulnerabilities that were introduced during their transformation efforts at the height of the pandemic.

CISOs are at a crossroads. To contend with the complex and draining issues they face, they must act fast. The chapters below outline what cybersecurity leaders need to know now about their current operating environment and what they need to do to transform it.

1. CISO at the crossroads
2. Three challenges holding back the CISO
3. Next steps for the CISO

CHAPTER 1

CISO at the crossroads

Over the last year, every business has had to adapt to disruption in one form or another. Within timeframes that would have been thought impossible just a short time ago, progressive organizations rolled out new customer-facing technology and cloud-based tools that supported remote working and kept the channel to market open.

But the speed of change came with a heavy price. Many businesses did not involve cybersecurity in the decision-making process, whether through oversight or an urgency to move as quickly as possible. As a result, new vulnerabilities entered an already fast-moving environment and continue to threaten the business today.

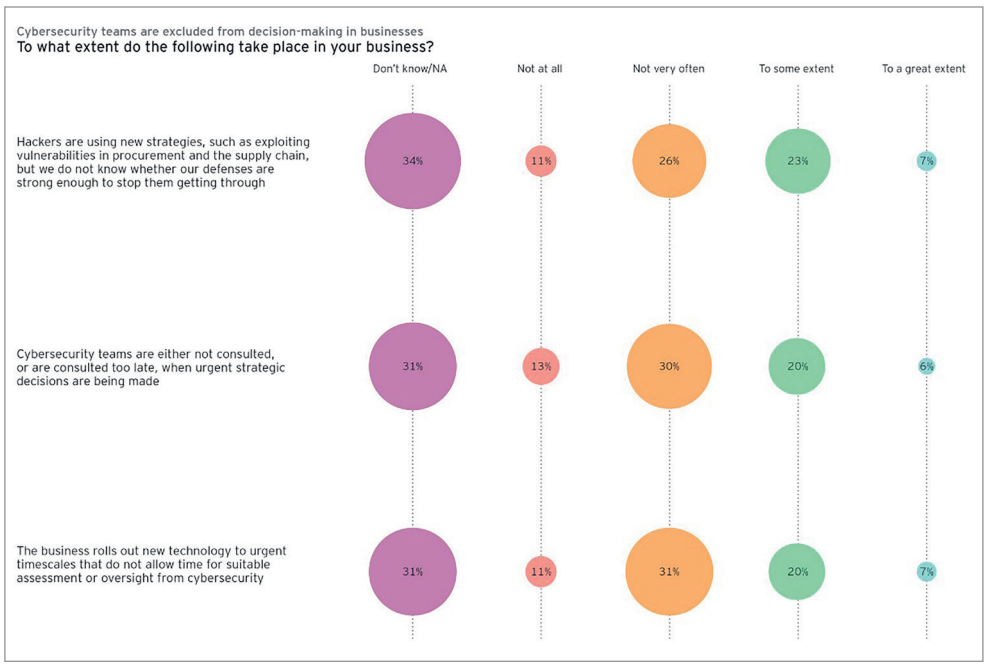
Rapid transformation brings new risks

At the time of writing, CISOs and their teams may not yet have completed a full assessment of the long-term impact that their company's new technology will have on its defenses. But in the meantime, it's likely that their colleagues are continuing to use the technology regardless.

"The urgency of the crisis meant that security was overlooked even while organizations were opening up systems that had never been open before," reflects Richard Watson, EY Asia-Pacific Cybersecurity Risk Consulting Leader. "Not all organizations acknowledge they now need to go back and address those issues."

The risks of moving on without addressing the issues are, however, very real and increasingly urgent. More than three in four (77%) respondents to this year's GISS warn that they have seen an increase in the number of disruptive attacks, such as ransomware, over the last 12 months. By contrast, just 59% saw an increase in the prior 12 months.

Yet CISOs are struggling to make themselves heard. Most respondents (56%) admit that cybersecurity teams are not consulted, or are consulted too late, when leadership makes urgent strategic decisions. While some maintain that this happens "not very often," it only needs to happen once for a flaw in the defenses to be exploited by threat actors.



The result is anxiety about what the future holds. "We strive for security as an enabler," says Richard Watson. "But there are still organizations that throw projects to security just before they go live."

At worst, CISOs find their warnings are ignored. In this year's GISS, 43% say they have never been as concerned as they are now about their ability to manage the cyber threat. But it does not have to be this way.

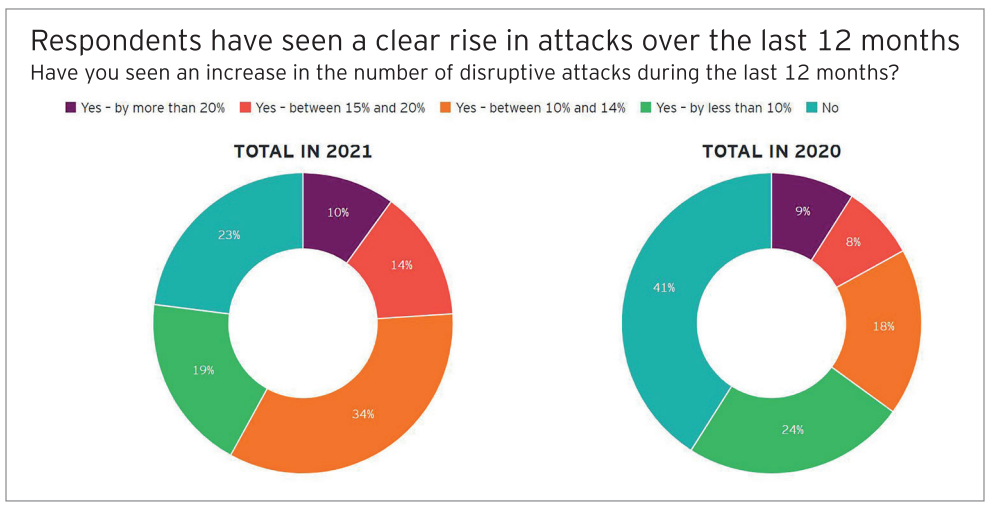
TikTok – Security by design, at speed

Roland Cloutier, Global Chief Security Officer (CSO) at short-form video and entertainment platform TikTok, is deeply involved in strategic decision-making on an iterative, week-by-week basis. "It may range from a strategy for user growth to a new type of monetization or music product," he says. "All involve the construction and distribution of new technology. I focus on understanding the implications of existing and unknown threats, and then add speed, security, and privacy by design into the product as it's built. Then I prepare the organization for the new information coming through. How do we do that at both the speed of the internet and the speed of culture? That's what makes this job so much fun."

Threat actors have hit a new level of maturity

Over the last year, threat actors have increasingly adopted new strategies, whether by targeting businesses with phishing campaigns containing malicious software that is forwarded by employees, or by embedding backdoor code that enables them to exploit commercial software after it has been procured by customers.■

(CONTINUED IN NEXT EDITION)



Cybersecurity, strategy, risk, compliance and resilience

EY Cybersecurity, strategy, risk, compliance and resilience teams can provide organizations with a clear picture of their current cyber risk posture and capabilities, giving them an informed view of how, where and why to invest in managing their cyber risks. It starts with better questions. The better the question. The better the answer. The better the world works. Please send an email to **isaac.sarpong@gh.ey.com** and copy in **kofi.akuoko@gh.ey.com**.

Find out more:

Address: 60 Rangoon Lane, Cantonments City, Accra.
P. O. Box KA16009, Airport, Accra, Ghana.
Telephone: +233 302 772001/772091
Email: info@gh.ey.com,
Website: ey.com