THE CYBERSECURITY GAP THAT TOP CEOs MISS

FEBRUARY 2021

THE CYBERSECURITY GAP THAT TOP CEOs MISS
FEBRUARY 2021

Public statements by CEOs, industry data, and private assessments by leading CISOs reveal a gaping hole in resourcing for 2025. We share 3 questions every CEO needs to ask their CISO to be prepared.

WHY ASK WHY?
FOR CEOS, IT'S PERSONAL (LIABILITY)

The accelerating pace of the cloud wars, and fast-tracked virtualization of work in the wake of COVID-19 have put increasing pressure on companies to take a proactive approach to who and how to allow access to their systems and data. After Target CEO Greg Steinhafel was forced to resign over a data breach, cybersecurity became part of the modern CEO's vocabulary. However, a 2020 KPMG study of 310 CEO's showed that only 1 in 8 saw cybersecurity as the greatest threat to their organization (after COVID-19) while at the same time, Gartner projected that 75% of CEOs would be personally liable for cybersecurity breaches by 2024! Are CEOs overconfident, are they concerned about signaling cyber weakness, or are CISOs truly keeping cyber risks at bay?

For nearly 20 years, BIA has analyzed executive statements – to identify behavioral signals -- using techniques originally developed for the CIA. The results have been validated by researchers at the Harvard Business School and profiled in The Wall Street Journal and Barron's. We applied our methodology to look at what CEOs and CISOs say about cybersecurity preparedness to understand whether CEOs and CISOs truly were confident in their cybersecurity strategy.

A LIE AND TWO TRUTHS…

When we look at cybersecurity pronouncements from CEOs, exchanges look something like this one between Adi Ignatius of Harvard Business Review and Jay Clayton, the CEO of Verizon, in April of 2020.

> Adi: With the heightened and urgent dependency on our communications infrastructure, what is the risk of disruption due to security threats, particularly as we're pushing toward peak capacity?
>
> Jay: To be honest, I think the peak mode is not the security risk here. All the risk is in the changed patterns. Much of corporate traffic, for example, has been at the office in the past. Now many company employees work from home or even on unknown Wi-Fi networks. That is posing a bigger cyberthreat at this moment.
>
> We serve 98% of the Fortune 500. That is a constant discussion I have with many of the corporations about how you secure that.

From a behavioral standpoint, we can confidently extrapolate that: (a) disruption is a bigger risk than Jay would like to admit, (b) he would like to imply that Verizon is a thought leader in securing WFH employee communications, and (c) he's not 100% confident Verizon is a leader in that space.

Let's compare that to two leaders who have license – and actually incentive – to be transparent about cybersecurity risks.

> Amit Yora, CEO of Tenable, was blunt, "In the past several months, we've seen cybercriminals take advantage of the current COVID situation."
>
> Jay Clayton, Chairman of the SEC, said in November that, "I know companies are burdened in many ways. Our registrants are burdened in many ways right now, but this [cybersecurity] is one of those things we just can't lose sight of." He went on to give specific guidance that companies and employees. For individuals, that means having strong passwords and multi-level authentication. For businesses, that means having multi-level backup systems, among other steps.

Why are those most vulnerable apparently the least transparent about their confidence?

LIKE SANDS IN AN HOURGLASS…

We interviewed CISOs at companies ranging from Series A startups to the Fortune Global 100, focusing on the security of endpoints where remote workers would access company networks.

Our CISOs reported full support of their CEOs and Boards for both cybersecurity as a priority and optimizing their posture for the short-term, even in the midst of the COVID-19 pandemic.

However, when discussing future roadmaps (beyond 2023), the picture became more muddy. Our CISOs broadly fell into one of three basic personas:

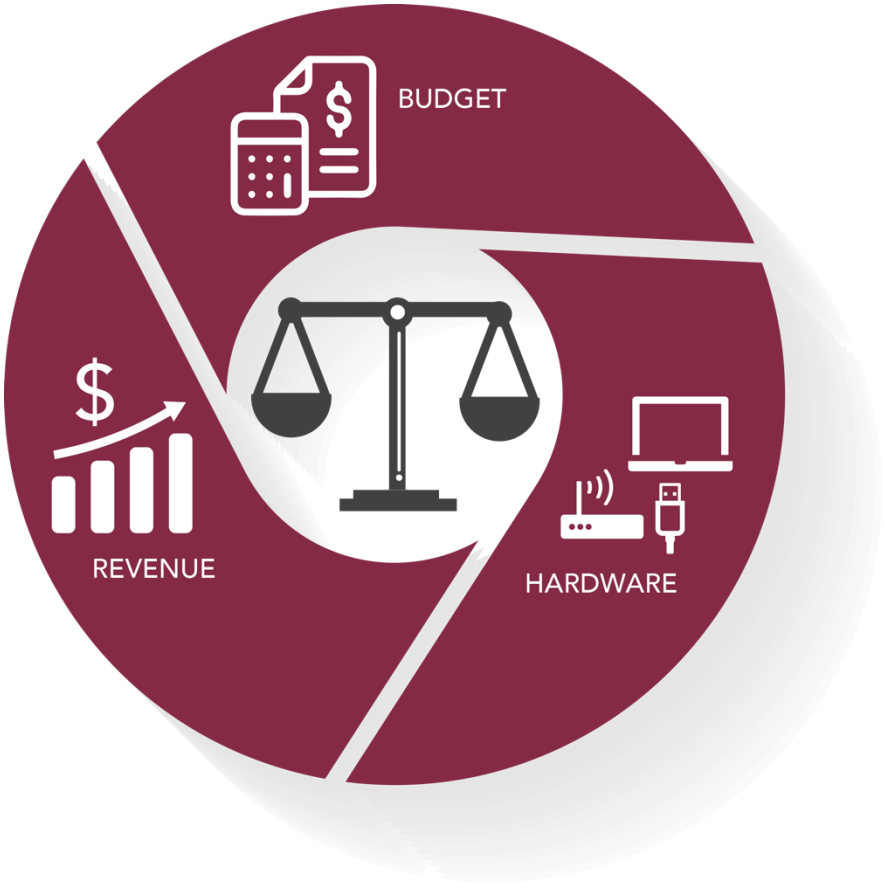
- Defensive CISOs, who seek to act as an internal security advocate and 'red team' for the CIO, prioritizing the fundamental security of the organization
- Offensive CISOs, who seek to innovate to reduce business friction while maintaining or increasing security.
- Operational CISOs, who reside somewhere between the Defensive and Offensive persona, prioritize increasing operating efficiency within the security architecture.

When we discussed pushback from their business counterparts on their long-term strategy, a full 50% of Offensive and Defensive CISOs and 100% of Operational CISOs exhibited behavioral signals that indicated resistance was greater than they were willing to disclose.

Why?

FORESIGHT IS 2025

The common threat across the C-suite was pushback in the intermediate term. Why? Behaviorally, this appeared to be centered on the uncertainty around where budget, hardware, and revenue constraints will fall. Today, CEOs and CISOs expressed a high degree of confidence that – given today's budget levels, hardware, and employee profile – their course of action was the right one and is a business reasonable solution for known risks.



When uncertainty was present, it appeared in subtly different ways the ability of the:

- CISO to make the case to 'move the goal posts' and get ahead of a security challenge when that perceived threat required exceeding the current budget and business posture and
- CEO to accurately dimension and advocate for those changes for 'hypothetical' risks.

These statements reveal a surprising gap in preparedness – a structural void that leaves businesses vulnerable to being a half step behind the state of the threat.

What can alert businesses do to avoid this looming professional (and, if Gartner is correct, personal) liability?

NEXT STEPS

The motto of the British Special Air Service (SAS) is “Who Dares Wins”, which is a fitting descriptor of the power of action over inaction. A common theme among CEOs and CISOs who showed high transparency and little reluctance to admit the difficult nature of cybersecurity were those who had clearly defined innovation programs looking at moving beyond traditional, “one size fits all” solutions. For Defensive CISOs, this typically focused on easy to adopt security-based solutions like true passwordless authentication solutions. For Offensive CISOs, this took the form of multi-sourcing vendor solutions for Authentication and Identification to allow greater control and optionality.

For leading organizations, certainty on the state of play in 2025 and beyond was irrelevant – the future would be uncertain, and as the landscape evolved, so would they.

What lesson can we take from these innovators?

FOR CEOs, ASK THREE QUESTIONS:

1. How would a CISO be able to notify the organization that the ‘game had changed’?
2. What steps have we defined/would we take to rapidly adapt toa new threat?
3. How accurately can we dimension the business impact of a threat?

FOR CISOs, ASK THREE QUESTIONS:

1. How aligned is the business with my guardrails to reevaluate our strategy?
2. If a guardrail is tripped, how prepared is the business to absorb the cost of action in an emergency (vs. pre-preparedness)?
3. Are my answers to #1 and #2 consistent with and symmetrical to #s 1 -3 for CEOs?

ABOUT THIS REPORT:

This report represents the application of BIA's Tactical Behavior Assessment® methodology and reflects BIA's assessment of the completeness and responsiveness of statements made during earnings conference calls, television interviews and other presentations. In each case, our assessment represents the opinion of BIA applying the Tactical Behavior Assessment® methodology and does not purport to indicate that any individual is in any specific instance being truthful or deceptive. BIA does not make stock recommendations. Under no circumstances is BIA's analysis intended to be a recommendation to buy or sell the securities of the company which is the subject of this report.

ABOUT BIA:

Business Intelligence Advisors (BIA) is the leading Intelligence Solutions research and advisory firm. Founded in 2001 on the principle that Intelligence techniques originally developed for the national intelligence community could be powerfully applied to the private sector, BIA has developed a ground-breaking suite of service offerings to provide clients with an edge in collecting and evaluating information critical to their success – whether that means making a more informed investment decision, identifying hidden risks, or enhancing due diligence efforts. BIA's services, which include proprietary Behavioral Intelligence Research, Expert Advisory, Investment Intelligence, and Learning & Development Solutions, are delivered by a team of in-house experts from the national intelligence and finance fields.

www.biadvisors.com