



AVERTIUM[®]

eBook

WHY THE TIME IS NOW FOR CISOS TO ADVOCATE FOR CYBERSECURITY IN THE BOARDROOM

(and how to do it)



| TABLE OF CONTENTS

Introduction	Page 2
So... Why Now?	Page 3
How CISOs can Make the Case for Cybersecurity as the PATH to Innovation - Not an Obstacle	Page 6
Create Internal Advocacy	Page 8
Conclusion	Page 10

INTRODUCTION

Historically, the average CISO has been **overburdened** and **undervalued**, tasked with a vast range of priorities that often compete with the priorities of the business (*as seen below*).

But today, the role of the **CISO** is changing.

As headlines become increasingly flooded with companies facing data breaches and ransomware attacks, the organizational perception of the CISO has shifted. Now, CISOs are seen as instrumental to not only the protection of the business, but also the *survival of the business*.

Organizational Goal: Scale the business as fast as possible.

CISO Goal: Take a proactive approach to information governance, keeping track of who has what data and where data flows within an organization.

Organizational Goal: Ensure that compliance mandates don't get in the way of doing business.

CISO Goal: Keep up with what's needed to maintain compliance, while advancing the maturity of the cybersecurity program.

Organizational Goal: Innovate. Be the most cutting edge in the market.

CISO Goal: Ensure that any and all innovation investments do not compromise the integrity of the organization's security infrastructure **WHILE** maintaining business continuity.

Organizational Goal: Increase profitability.

CISO Goal: Mitigate risk.

| SO... WHY NOW?

Reason #1: Rise in Cyber Attacks

The increase in cyber attacks has helped people better understand the value and importance of cybersecurity.

Both private and public organizations have faced an alarming rise in cyber attacks within the past year. These attacks have not only become more frequent, but the tactics, techniques, and procedures (TTPs) have also evolved.

- Malware increased by 358% overall and ransomware increased by 435% as compared to 2019. ([Source: Forbes](#))
- Google has registered over 2 million phishing sites as of January 2021. This is up from 1.7 million in January 2020, which equates to a 27% increase in 12 months. ([Source: Forbes](#))

Prior to this year, many companies believed that the likelihood of a cyberattack impacting them was relatively low. But as each mainstream news headline emerges chronicling the latest ransomware attack, this attitude is shifting. US companies have been hit particularly badly this past year, with major attacks such as the [SolarWinds' Orion attack](#) and the [Colonial Pipeline attack](#) causing major disruption for everyday people.

The rise in cybercrime is well documented, and more and more people are beginning to pay attention to cybersecurity, which has increased the demand and perceived value of cybersecurity professionals. According to [the State of the CIO study](#), 40% of IT leaders say cybersecurity job positions are the most difficult to fill.

So what does this mean? It means that CISO's are no longer the only people in a business rooting for cybersecurity.



Phishing increased by **27%**

Malware increased by **358%**

Ransomware increased by **435%**

Related Readings:

1. [Flash Notice: SonicWall Warns of Imminent Ransomware Attack Against EOL Products](#)
2. [Blog: J&J experiences 15.5B cybersecurity incidents per day, CISO says](#)
3. [Blog: Insurance giant CNA hit by new Phoenix CryptoLocker ransomware](#)

Nothing gets the c-suite and board's attention like shutting off the revenue spigot.

“Security strategy is mainstream because information security is now more than compliance and a public black eye. In the good old days, a security breach might result in monetary fines, negative publicity, and worst-case, lawsuits from people who's data was breached. *The new normal is that ransomware (and other system-disrupting attacks) have proven to be profitable for the attackers.* Fines and legal settlements are not existential threats to running a business, shutting down production is. Nothing gets the c-suite and board's attention like shutting off the revenue spigot.”

Joseph R. Thomas | CISO

myNEXUS 

Reason #2: Geopolitical Dynamics

The US has its eye on cybersecurity now more than ever.

Politics has become a central driver of the increasing prevalence and sophistication of cyberattacks. [Attacks based out of Russia](#), China, and Turkey have grown more frequent, pushing the US to take new measures against these digital assaults, including a recent [executive order](#) from the Biden administration that emphasized the necessity of prioritizing cybersecurity in protecting both public and private institutions from cyber threats.

While the order itself was aimed at the public sector, the idea that cybersecurity was highlighted in an executive order signals that security is no longer a nice-to-have, but an absolute necessity.

Attacks based out of Russia, China, and Turkey have grown **MORE FREQUENT**



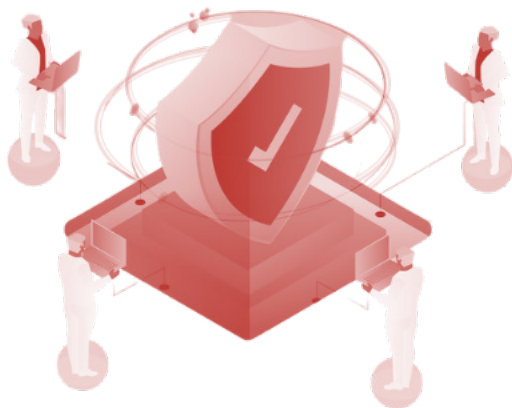
Reason #3: COVID Impact

The global pandemic has been a huge driver in the shift in attitudes toward cybersecurity as well.

Virtually every company had to contend with the move to remote work environments, when pretty much overnight, organizations tripled the size of their attack surface.

This created massive opportunities for bad actors to infiltrate companies' networks, which had major implications for pretty much every aspect of cybersecurity.

So yes, cybersecurity now stands at a pivotal place within the market. In the past, SecOps have always been looked at as a cost center, and CISOs as a blocker to innovation. But in this present moment, CISOs have an opportunity to elevate the perception of cybersecurity function from a cost center to a strategic priority. CISO/CSOs can now work closely with business teams (in addition to leading SecOps) to enhance an organization's overall cybersecurity resilience.



Security is a simple formula of “likelihood times impact”, you have to work both sides all the time.

“The one question I’ve always gotten from the board is, ‘*Are we 100% secure?*’, my answer will always be, ‘*No, we will never be 100% secure, but we will always be 100% ready.*’ We can put together graphs and metrics all day long but that is really what the board cares about, are we doing everything we can and are we ready to react to reduce the impact as much as possible. Security is a simple formula of ‘*likelihood times impact*’, you have to work both sides all the time. *Focusing exclusively on impact over a likelihood of an incident or vice versa is short sighted, both equally are important to risk reduction.*”

Keith O’ Sullivan | SVP, IT Risk & Chief Information Security Officer

standard

Related Reading:

1. [How to Protect Workers from Increased Phishing Attacks During COVID-19](#)

HOW CISOS CAN MAKE THE CASE FOR CYBERSECURITY AS THE PATH TO INNOVATION – NOT AN OBSTACLE

Quantify the potential value of investing in cybersecurity... as well as the cost of inaction.

Tactic 1 – Position Cybersecurity as a Sales Tool

In business, everyone is looking for that competitive edge. And in today's chaotic threat environment, cybersecurity could be yours. With third-party risk on the minds of many, you can also leverage your cybersecurity posture to create hesitation in the minds of your prospects with regard to competitors.

Because in the eyes of prospects, potential partners, and current customers, strong cybersecurity hygiene equates to [trustworthiness](#).

Tactic 2 – Quantify the Hard Costs of a Breach, Highlighting the Risks

While the true cost of a breach isn't measured in just a ransom payment, that payment could be enough for CISOs to make the case for more company resources dedicated to cybersecurity.

These costs are difficult to measure at the individual business level, but here are a few stats to ponder:

- The value of ransom demands has gone up, with some demands exceeding over \$1 million. ([Cybersecurity & Infrastructure Security Agency, 2021](#))
- In 2021, the average payout by a mid-sized organization was \$170,404. ([Sophos, 2021](#))
- On average, ransomware attacks cause 15 business days of downtime. Due to this inactivity, businesses lost around \$8,500 an hour. ([Health IT Security, 2020](#))
- The hacker group behind an oil company attack allegedly acquired \$90 million in ransom payments in only nine months from around 47 victims. ([Fox Business, 2021](#))
- Cybersecurity Ventures predicts that ransomware will cost \$6 trillion annually. ([Cybersecurity Ventures, 2020](#))

That said, discussing the potential costs of a breach is much more impactful when contextualized alongside the risk of a breach actually happening.

For example, according to [Verizon's Data Breach Investigations Report \(DBIR\)](#), 94% of malware is delivered via email. The impact of highlighting potential costs is only amplified when positioned alongside the fact that it only takes a single email to unleash absolute chaos.

While breaches can happen to anyone, small and mid-sized organizations are particularly vulnerable to breaches, as they often don't have the resources to allocate toward enterprise-level cybersecurity. And unfortunately, the financial impacts of a data breach can be much more detrimental to the survival of small to mid-sized organizations with finite resources.

Small to mid-sized businesses are the low-hanging fruit for hackers.

“Small to mid-sized businesses are the low-hanging fruit for hackers. It's common for many of these business owners to *dramatically underestimate their cyber exposure and the financial costs* associated with hacking attacks. If you don't have the resources to effectively respond to one of these events, *the fallout can be absolutely devastating.*”

Patrick Costello | Co-Founder & Principal



Tactic 3 – Illustrate the Potential Ripple Effects of a Breach

With any cyber attack, the hard dollar costs are just the beginning... and it's important that company stakeholders understand the ripple effects that come from a cyber attack, including:



Business reputation + brand equity loss:

Third-parties, vendors, and partners are less likely to want to work or be associated with a company that may have been deemed unsafe in an industry. They will not want to risk their own assets to work with a compromised company.



Operational downtime: When a breach occurs, your company will not be able to continue as if things are normal. Oftentimes, networks must be shut down to contain the attack before it spreads. Ask leadership: “How long could we withstand that kind of sustained disruption?”



Loss of customers: Customers do not want to risk having their sensitive data stolen and will absolutely leave if they believe you are not a trustworthy company. And the easiest way to have a breach of trust with customers is to have a breach of data...Which means a direct impact on your company's bottom line.

These ripple effects add up. According to a [2021 Sophos report](#), the average cost to recover from a ransomware attack is \$1.85 million. To accurately quantify these risks with respect to your organization, it might make sense to perform an assessment or bring in a third party for audit services in order to illustrate all of the vulnerabilities within your company that executives may not even know about.

Tactics on how CISOs can make the case for cybersecurity as the PATH to innovation — not an obstacle:

1: Position Cybersecurity as a Sales Tool

Because in the eyes of prospects, potential partners, and current customers, strong cybersecurity hygiene equates to trustworthiness.

2: Quantify the Hard Costs of a Breach, Highlighting the Risks

Discussing the potential costs of a breach is much more impactful when contextualized alongside the risk of a breach actually happening. The impact of highlighting potential costs is only amplified when positioned alongside the fact that it only takes a single email to unleash absolute chaos.

3: Illustrate the Potential Ripple Effects of a Breach

It's important that company stakeholders understand the ripple effects that come from a cyber attack to better illustrate all of the vulnerabilities within your company. The ripple effects — business reputation + brand equity loss, operational downtime, and loss of customers — add up.

KEY POINTS

| CREATE INTERNAL ADVOCACY

Tactic 1 — Get in early and stay involved throughout the digital transformation conversation.

The CISO/CSO and SecOps team are aware of the challenges they're up against and how not acting accordingly could impact the company. Getting that message across to internal stakeholders in a way that's actually understood? That's where the real challenge lies.

As companies begin the digital transformation conversation, it's important for CISOs to have a seat at the table. Cybersecurity professionals don't have to feel like a buzzkill to the rest of the company. Claiming your seat at the table and using it to communicate that you're not there to say no to innovation and instead there to explain how to get to yes safely will go a long way.

Tactic 2 — Try to do some of your own internal marketing for cybersecurity.

Creating a culture of cybersecurity within your company requires influence. Relationships are critical, so knowing your executive team and being able to talk to them about cybersecurity in a way that resonates with them is key. That's why it's important to frame the conversation in the context of who you're talking to and what their goals are.

For example:



When talking to **marketing stakeholders**, it might make sense to talk about customers who are choosing to go with brands who prioritize cybersecurity, or how brand reputation suffers in the event of a breach.



When talking to **financial stakeholders**, it's all about the dollars and cents. Therefore, quantifying the potential earnings lost from a ransomware attack or presenting a cost-benefit analysis on cybersecurity investment might be an effective way to get them on your side.



When talking to **company leadership or board members**, you'll want to focus on the big picture benefits of cybersecurity investment and highlight how it mitigates business risk. Moreover, having a target state and clear milestones will go a long way in solidifying your points in a way that resonates with them.

Tactic 3 — Benchmark your cybersecurity investment against peers.

Comparisons are a powerful tool in the business realm.

- What are your competitors doing?
- How much are they spending?
- How does that compare to what your company is doing?
- Does leadership really want to lose the cybersecurity game in a moment when cybersecurity is top of mind for so many businesses?

While this information is not readily available, you might be able to get an idea of what other companies are doing just by talking to your peers. At business events, conferences, and other professional settings, you can talk with colleagues and ask questions about how they're approaching their cybersecurity strategy.

Tactic 4 — Don't just bring problems. Bring solutions.

It's worth repeating: CISOs must position cybersecurity as the safe path to innovation — not a blocker.

Instead, CISOs should bring alternative solutions to the table, emphasizing clearly and concisely how to reach company goals while mitigating cybersecurity risk. Identify a target state. Incorporate milestones and quantitative ways to measure progress. Most importantly, illustrate how cybersecurity plays into organizational goals in a way that's understandable and accessible to non-cybersecurity professionals.

Tactics on how CISOs can create internal advocacy:

1: Get in early and stay involved throughout the digital transformation conversation.

Claiming your seat at the table and using it to communicate that you're not there to say no to innovation and instead there to explain how to get to yes safely will go a long way.

2: Try to do some of your own internal marketing for cybersecurity.

Relationships are critical, so knowing your executive team and being able to talk to them about cybersecurity in a way that resonates with them is key — frame the conversation in the context of who you're talking to.

3: Benchmark your cybersecurity investment against peers.

Comparisons are a powerful tool in the business realm. And while this information is not readily available, you might be able to get an idea of what other companies are doing just by talking to your peers.

4: Don't just bring problems. Bring solutions.

On top of illustrating how cybersecurity plays into organizational goals, CISOs should bring alternative solutions to the table, emphasizing clearly and concisely how to reach company goals while mitigating cybersecurity risk.

KEY POINTS

| CONCLUSION

At the end of the day, companies want to know what the problem is and how it can be solved. This is something a CISO should be able to do once they get their audience's attention.

For CISOs who live and breathe cybersecurity every day, it's easy to fall into the trap of inundating non-cybersecurity professionals

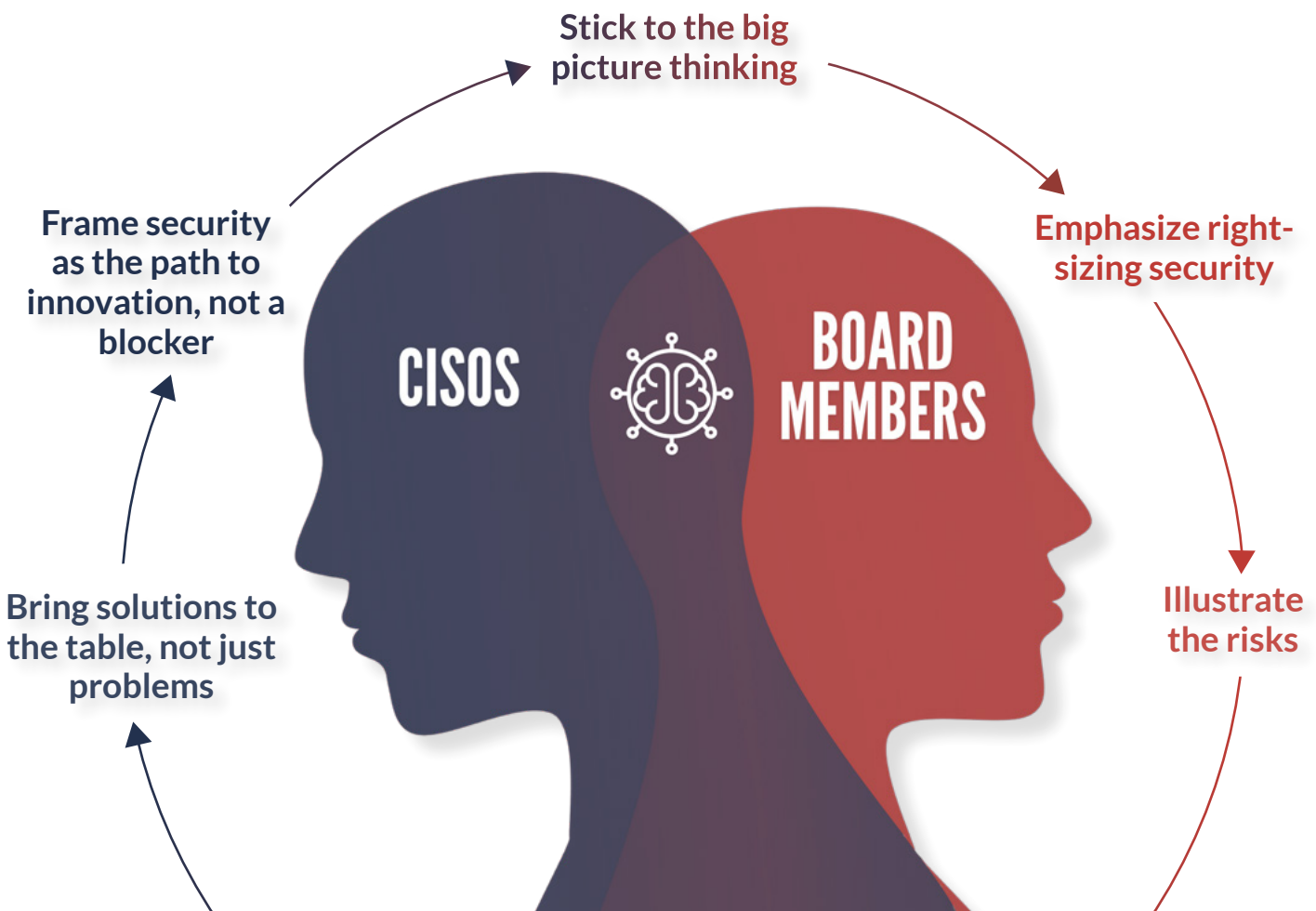
with technical jargon that detracts from the larger point you're trying to make. If CISOs come into every conversation using this technical jargon, their message will not stick with company stakeholders and thus, no progress will be made. **That's why it's important to simplify what you need to say and deliver with confidence.**

CISOs can advocate for cybersecurity more effectively by remembering the following:

1. **Stick to the big picture thinking** – Your company stakeholders want to know: Are we safe from ransomware? How can we achieve cybersecurity resilience without compromising business continuity?
2. **Emphasize right-sizing security** – Company leadership wants to trust that they’re getting everything they need in order to mitigate risk, and nothing they don’t. Distinguish the “must-haves” and the “nice-to-haves.”
3. **Illustrate the risks** – Talk about emerging threats, how they apply to your organization, and highlight the gaps in your security program that could potentially lead to major incidents.

4. **Bring solutions to the table, not just problems** – After describing the issue, follow it immediately by offering a path to remediation with clear milestones. Be prepared to answer questions.
5. **Frame security as the path to innovation, not a blocker** – Frame the conversation as, “If we make this investment, we’ll be able to...”

Don’t wait for a crisis to learn where your points of vulnerability are – have the conversation now. Gather an internal team or enlist the right partners to help you know yourself, know your enemy, adapt, protect, and evolve.




ABOUT AVERTIUM

Avertium is the security partner that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity - one that drives action on the ground and influence in the boardroom.

That's why over 1,200 mid-market and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective, and more resilient when waging today's cyber war. Show no weakness.®

CONNECT WITH US



 Cyber Fusion Centers of Excellence
Arizona • Colorado • Tennessee

 Contact Us | www.Avertium.com



This publication contains general information only and Avertium 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 advisor.

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

Copyright © 2021 Avertium. All rights reserved. | [Privacy Policy](#)

SHOW NO WEAKNESS.®