AMERICAN CISO

Dealin’ with cyber in a star-spangled manner!
INTRODUCTION

In 2020, the US cybersecurity market size was valued at $58.5 billion, taking the lion’s share in a global market size of $167.13 billion (source). The United States is also the country suffering the highest average total cost incurred by data breaches - a national cost of $8.64 million vs. the global average of $3.86 million (source).

It’s no wonder then, that the second-highest paying tech job in 2019 is the CISO, with a salary range of $175,000 to $275,000. CISOs of Fortune 500 corporations in the big cities of the US get paid as much as $380,000 to $420,000 annually (sources: 1, 2).

These US-based CISOs are significantly out-earning other countries: median UK CISO salary is $129,627, French is €117,972. Even strong financial centers like Hong Kong ($234,471), Singapore ($169,075) and Dubai ($133,409) fall behind (source).

This begs the question: Why? Why do American CISOs in the land-of-the-free make so much money compared to the rest of the world?

The obvious answer is simple market forces: market size, supply and demand etc. But I’d like to suggest an additional line of thinking: The CISOs job is notoriously hard, demanding, and stressful. The responsibility is huge, and there is little-to-no margin for error. This is the nature of CISOs work all over the world - heavy is the head that wears the crown.

However, two things that are deeply ingrained in the DNA of American corporate culture might shed light on the matter: liability and accountability.

Being the top-dog means ownership - of processes, technology, budget, and, of course, results.

Ownership in its american sense is a double edged sword: You are the top dog and you earn as such. You "get a say". You “shape the future security posture of the organization”. On the other hand, you are the one to take the fall the minute the you-know-what hits the fan - that’s accountability. If that’s not enough, you are exposed to legal actions from the board of directors - that’s liability. CISOs need extra nerves of steel: Their minds are constantly busy in staying ahead of threats, compliance, workforce issues, and their boards.

We talked with American CISOs of organizations of different sizes, from various industries, and , as the calls unfolded, patterns or themes emerged. We hope that by providing a sneak-peek into the minds of executives at the top of the cyber food chain, you will gain perspective, insight and inspiration to drive the change you want to see in your organization’s cyber operations and propel your career forward in the relentless pursuit of confidence.

Yours,

Lior Marom, CISO, Cybersixgill
We spoke with numerous American CISOs from companies of various sizes and industries - see what they had to say.

The purpose of this eBook is to provide valuable insight into the perspectives of US-based CISOs across several industries. More importantly, these observations are intended to help Cybersecurity executives such as yourself determine what needs to be done in your own organization to maximize the efficiency of cybersecurity programs and the return on security investment.
Awareness

The top priority across the board is investing, raising and promoting cybersecurity awareness across the organization and beyond.

• “Board awareness” is a thing.
  What are your KPIs? How much information should you share with the board? Keep in mind, they are interested in supporting the business. So, less FUD, more focus on value and progress.

• With 3rd party risk becoming a major threat, the need for cyber awareness, training and education for vendors is crucial for minimizing cyber risk.

• Employees’ awareness of the potential risks, threats and how to minimize it is essential for organizational cyber-hygiene.

Investments in cybersecurity awareness to enable the workforce

“Basically, we would like to create a culture of cybersecurity. We will focus on building an education program (already started) that needs to orient our planning around the skills and competencies critical for success in the new digital era.”
Investments in cybersecurity awareness to enable the workforce

"Cybersecurity awareness for global workforce: Cybersecurity training and emphasizing the importance of being vigilant to recognize threats is critical to the infrastructure of any e-commerce venture."

We are expecting that the cyber awareness training which we have developed in-house and also in collaboration with external trainers will be adapted both to cover remote-work situations and bring-your-own-device policies and will be delivered virtually.

And also for the board

"Enhancing internal reporting risk and security to the board execs: keeping the top executives aware on critical and emerging risks. This also helps us reallocate funds to digital innovation from many non-essential projects."

"...Make sure our third party partners, suppliers and employees should be provided opportunities for continuing education and be regularly briefed on company’s cybersecurity policies."

learn more here
As a leader responsible for information security, I think the top priority for me is focusing on training my team on automation, networking, security, AI, and digital collaboration, building strong internal capabilities and security skill sets.”

Agility

Respondents also expressed the importance of agility. In order to achieve this, security professionals must implement modern, continuous, iterative, and smarter methodologies, tools and processes. This is essential in order for cybersecurity teams to effectively digest the rapidly increasing amount of data, reduce knowledge and workforce gaps, and maximize teams’ performance.

Agile threat intelligence is the driver of accelerated cyber operations. Analysts achieve more - faster. When teams cooperate in an effective manner, executive leadership can coherently see the big picture, understanding the risks as well as the steps being taken to mitigate them.
The agile cycle - example

A threat actor had created a malware and distributed it on the dark web: Traditional threat intelligence feeds will detect the new malware only once the malware is sold and weaponized, or worse, when the attack has already happened. When taking a CI/CP approach, you shift left and:

- **Detect** the malware when it is initially offered for sale on the dark web.
- **Extract** the malware hash in the preliminary phase.
- **Block it** on your FW, trigger playbooks on your SIEM, SOAR, EPP, or VM platforms **before anyone has even downloaded it.**
- **Understand** who authored the malware that was targeting you: determine the threat actor’s motivations, TTPs, social network and patterns in order to assess their next steps.

With the information at your fingertips, you can now take the appropriate actions to ensure your organization’s security.

Learn more how Cybersixgill integrates with your security stack [here](#).
The Impact
Your teams will combat the incoming threats faster and in a more scalable way than ever before:
- Leveraging more relevant data
- Faster, more accurate detection
- Data is matched with specific playbooks on your SOAR/SIEM
- Cross-teams collaboration for overall better performance

The Key
The key here is to embrace automation with a grain of salt - a human being is still in the loop and still has authority over the outcome, yet they are supercharged with the brainpower of the machine.

Agility is also a goal at the board level

“One thing which remains constant is agility and fast response to every situation with a reliable solution. We keep our internal and external security threat reports very transparent and timely so that the board is aware of the problems and our response.”
The evolution of threat intelligence

No SOC or threat intelligence
Your organization is new and still focuses on IT ops alone.

Naive SOC
Still drawing on the walls of the SOC, going through incidents, but not leveraging threat intelligence.

Free feeds, generic reports
Your organization is taking action based on basic legacy and commodity threat intelligence, but note that it is probably outdated and is being updated in long cycles. You will most likely not be able to track real-time threats that specifically target your organization.

Paid feeds, PIRs as a basis for reports
Your organization is taking action based on threat intelligence specific to your attack landscape, yet still, you are only fixated on the things you know to look for. You are reactive, not proactive, and you can’t scale your operations.

Proactive (yet manual) searches on the cybercrime underground
Your organization is taking action based on threat intelligence specific to your attack landscape in a proactive manner, but there is no chance you could analyze all the data that is out there manually. You are only able to take care of a small fraction of the data, whether these are IOCs or posts from the Dark and Deep Web.

Proactive (yet manual)
searches on the
cybercrime underground

Agile: Cybersixgill feeds and Investigative Portal
Your organization is using all the right tools - you are proactive and able to tackle all the threats you meet, but the data still doesn’t flow smoothly in your organization. You do not have one narrative for all of your teams, and you are probably facing balkanization. Let’s fix it!

Agility means being predictive as well as proactive

“Security programs need agile management to not only respond, but also have ability to predict and protect.”
Implementing CI/CP™ with Cybersixgill

Investigative Portal
- Quickly deep dive into any escalation in real-time and get the complete picture to understand the context
- Review and analyze across languages, sites, timeframes, types of products, topics, entities, and more
- Get real-time actionable alerts customized to your needs and interests

Intelligence Backbone
- 7x detection of leaked credentials
- 10x collection from dark web sources
- 13x collection from instant messaging apps
- 24x faster extraction

Feeds
- Unique and advance warnings about new cyberthreats: malicious IOCs, prominent CVEs, and more
- Contextual and fully automated (machine-to-machine)
- IOCs are delivered in real-time and are actionable

Automation is key

"We expect third party service providers to make up for increased workloads by adding automated processes such as security alerts and automation response tooling rather than by increasing internal staff or budgets."

Retail
- 30,000-49,999 employees
- $10 BN annual revenue

Let’s talk about it Speak to an agile expert
Cybersecurity and compliance are often intertwined as CISOs have to consider any regulatory mandates that may affect the organization’s cybersecurity posture.

COVID-19 accelerated what was already happening organically - the shift to “work-from-home”. This increased organizations’ risk posture ten-fold almost overnight, and with it, the need for scaling cybersecurity operations. Digesting this amount of information whilst remaining in-line with regulations can exhaust tremendous resources - unless you take the necessary steps to harness automation and implement agile methodologies.

Global presence demands local compliance

“Having presence in multiple regions also requires all certifications and compliance standards are met.”
Compliance is a major concern when scaling IT operations. One of the key challenges that I foresee, for now, is scaling up our internal IT infrastructure while adhering to security standards and compliance, also ensuring all remote working frameworks are in place.

How automation of threat intelligence allows scaling SecOps

**A whole new level of visibility**
Deep understanding of threat actors’ mindset, connection expertise, motivations, and M.O.s, enabling security teams to better anticipate, intercept and respond to incoming threats.

**Real-time gets real**
A continuous stream of valuable intelligence that seamlessly adjusts itself to the changing nature of the threat actors’ ways of communication, allowing SecOps to keep up and even stay ahead of threats.

**Breaking silos**
Teams are constantly and proactively responding to the most updated intelligence picture, generating fresh, relevant intel to take incident detection, prevention and response to the next level, with minimum business interruption, thereby maximizing the performance of people, platforms and processes.

**New ways to save the day**
Tackling challenges you could not before (like shadow IT risks, lag-times, and visibility issues), simply due to the amount of data your teams had to digest.

To learn more how CISOs use Cybersixgill’s solutions click here.
Basic requirements

Real-time collection mechanism
gives you an exclusive access into the darkest corners of the underground.

Predictive feed of IOCs
curated from the underground in a contextual way that will allow you to act upon it.

Investigative portal
to slice and dice the data and investigate escalated incidents with minimum effort.

Integration with your security platforms
to enable a seamless response with each intel development.

Privacy is a main engine for compliance in insurance.

"Compliance is always a big challenge to keep track of. Especially, when consumers continue to demand that their privacy be protected. To tackle this we are further exploring options and evolving our privacy management program with focusing on ever-growing compliance.”
So much it can affect mid-year budget changes

"One more scenario which can impact the mid-year budget is any change in privacy and compliance regulations."

Additional resources - where to go from here

**Threat reports** - Read more about cybersecurity risks across different industries and ways to overcome them

**CISO survey** - We interviewed 150 CISOs from various industries - learn what’s on their minds

**The Cybersixgill blog** - Everything that is threat intelligence
About Cybersixgill

Cybersixgill’s fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response - in real-time. The Cybersixgill Investigative Portal empowers security teams with contextual and actionable insights as well as the ability to conduct real-time investigations.

Rich data feeds such as Darkfeed™ and DVE Score™ harness Cybersixgill’s unmatched intelligence collection capabilities and deliver real-time intel into organizations’ existing security systems. Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities.

some of our clients:

To learn more how Cybersixgill solutions can help your organization Proactively Protect And Maximize Security Investment With Intel That Makes An Impact email:
info@cybersixgill.com