The 1st Global

Cybersecurity Observatory

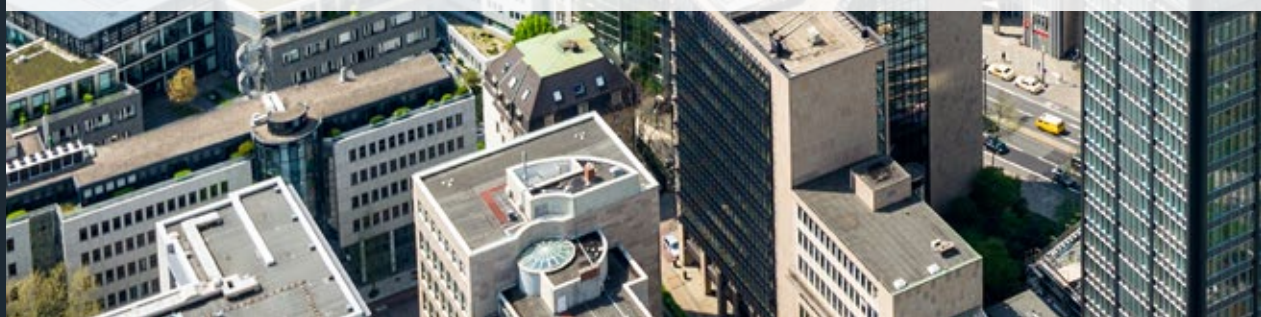
cyberstartupobservatory.com



Europe

Second Edition

November 2020



Leadership



Branko Džakula

CISO
at
Kaia Health



Branko Džakula

CISO at Kaia Health

Branko first felt the passion for the field back in 2010 working on private projects and started his cyber security career in the TelCo industry.



Through years of frontline battles with cyber criminals his career led him to Information Security Management and gave him a chance to have a bigger influence on an organization-wide security program and its maturity - which he says gave him a bigger family to take care of.

Through Airlines, SaaS, OTA and Healthcare industries he has seen all the shapes and sizes cybercrime comes in and experienced first-hand how to fight it face to face.

The job of CISO is never going to be an easy one, no matter what you do. The bad guys only have to be right once. How do you deal with that when it seems like an impossible challenge?

This is a harsh truth of our job and the weight of it is not easy to carry. However, there are ways a CISO can deal with it - it just depends on the personal preference. I, myself, look into it from the simple philosophy of the Stoics, meaning in a very high-level sense that we should not worry about the things out of our control and give our best for the things that are.

This balance ensures the highest level of commitment in doing your work and still keeping a cool head when the worst happens; this is the time when everyone will count on you to be the voice of reason and to lead them through the storm. I have had my share of storms and it gets easier over time.

"This is the time when everyone will count on you to be the voice of reason and to lead them through the storm. I have had my share of storms and it gets easier over time."



What can help a CISO be prepared is practice, even just a mental practice of a hypothetical data breach scenario. It keeps the mind at ease and ready for anything. Naturally, what I highly recommend is a proper and rehearsed incident response plan with specific scenarios involving a data breach level threat.

How important is it to have the CEO thinking that security matters?

CEOs have to lead by example for security to work as they are steering the ship - that is their responsibility. We are the first officers and there to execute what our leader sees fit for the organization’s continued success. If one of those things is not a commitment to care about security and privacy, the CISO is doomed to fail.

Almost everybody agrees that organizations need a culture of security. How can security leaders help facilitate that type of culture?

CISOs have to be great communicators, educators and true ambassadors of their practice in order to perform a cultural shift towards security and privacy first mindset. Knowledge is important but the right attitude is what wins the battle.

What should a company do if it suspects cyber attackers have been successful?

Execute its incident response plan/ crisis management plan, gather relevant team members and perform a full-scale investigation. At this point data is everything and it will steer the way you respond to this situation with informed decisions.

What companies should NOT do is try to hide any evidence of a confirmed data breach, try to stay silent and hope it all goes away.

CISOs should have an ethical responsibility to stand for just security practices and the right to personal data privacy, and users have the right to know and be warned if their data is now in the hands of cyber criminals, even if it means the company would suffer a financial hit and reputational loss.

But the reality is the opposite - being honest and transparent is what ensures the highest user retention rate post Data breach, and minimal financial and reputational loss. Stay honest and transparent.

How can CISOs / Leaders balance security and innovation?

This can be achieved with the following mindset: security has to be convenient. Looking at security practices, processes and principles this way, your organization's culture shifts the thought process towards solutions that are truly innovative, secure AND convenient. Security should never be a blocker, but an enabler.

How important is being able to communicate with your colleagues?

It is imperative in the world of security. Successful security-aware culture depends on timely communication and accessibility of their security team members and their CISO.

I always end my security awareness training with - there are no stupid questions, whenever in doubt send me a message or give me a call, you just might prevent a next company disaster. Communication is everything.

Closing statement

Being a CISO is not for everyone, it takes its toll, but it has its rewards too.

It tests your character on a daily basis, it puts you into uncomfortable situations instead of a good morning and it gives you responsibilities that can dwarf your common life problems - but it gives you the reassurance that you are playing for the right team, making this new digital world a bit better and safer every day.

It's a hell of a job, it sucks, and I love it!

