YL VENTURES
The CISO Current

The CISO Current Report

Q4, 2019

About YL Ventures

YL Ventures funds and supports Israeli tech entrepreneurs from seed to lead. Based in Silicon Valley and Tel Aviv, the firm currently manages $260 million and exclusively invests in cybersecurity.

YL Ventures' focused strategy allows it to conduct a rapid and efficient evaluation process and support each of its portfolio companies, both strategically and tactically, across multiple functions post-investment. The firm is uniquely focused on supporting the U.S. go-to-market of early stage companies and leverages a vast network of industry experts, CISOs, and U.S.-based technology companies as advisors, prospective customers, and acquirers of its portfolio businesses.

The firm's global network and footing in the U.S. have always counted among its most powerful assets: YL Ventures bridges the gap between Israeli innovation and the U.S. market. The firm has formalized and amplified this core competitive advantage through the launch of YL Ventures' Venture Advisory Board.

YL Ventures' Venture Advisory Board is comprised of over 70 security professionals from leading multinationals, including CISCO, Walmart, Netflix, Nike, Spotify, Wells Fargo, Julius Baer, Aetna, and more. The firm's relationship with its advisors, as well as its extended network, is symbiotic in nature: the advisors bolster the YL Ventures investment due diligence process and provide the firm's portfolio companies continuous support across a multitude of functions throughout their life cycles. In return, network members benefit from exposure to pre-vetted Israeli cybersecurity innovations and receive direct exposure to a market second only to the U.S. in cybersecurity innovation.

Portfolio

cycode
Source Code Control, Detection, and Response Platform
www.cycode.com

orca
Full Stack Cloud Visibility Platform
www.orca.security

Hunters.
Autonomous Threat Hunting Platform
www.hunters.ai

VULCAN mind the gap
Continuous Vulnerability Remediation Platform
www.vulcan.io

MEDIGATE
Securing the Internet of Medical Things
www.medigate.io

AXONIUS
Cybersecurity Asset Management Platform
www.axonius.com

Karamba Security
Embedded Security for Connected Systems
www.karambasecurity.com

Acquisitions

Twistlock
Acquired by
paloalto NETWORKS

HEXADITE
Acquired by
Microsoft

FIRELAYERS
Acquired by
proofpoint

Seculert
Acquired by
radware Every second counts

BlazeMeter
Acquired by
ca technologies

clicktale
Exited to
Amadeus Capital

AcceloWeb Click. You're there.
Acquired by
Limelight NETWORKS

UPSTREAM COMMERCE
Acquired by
Walmart

About the CISO Current

YL Ventures frequently confers with an extended network of prominent cybersecurity professionals, including our Venture Advisory Board and industry executives, to assess our portfolio prospects, inform market predictions, and cultivate portfolio company business development.

As such, we have established direct lines of communication with the global market's preeminent CISOs and cybersecurity experts for ongoing insights into their thoughts, priorities, and opinions about the state of their organizational cybersecurity. We recognize the value this information presents to entrepreneurs, especially those wishing to enter the U.S. cybersecurity market, and to the cybersecurity community as a whole. For this reason, YL Ventures launched 'The CISO Current', an initiative under which we publish reports containing gathered intelligence for general use.

We hope the observations compiled in this report will prove a useful resource for aspiring cybersecurity entrepreneurs and the rest of the cybersecurity community.

Table of Contents

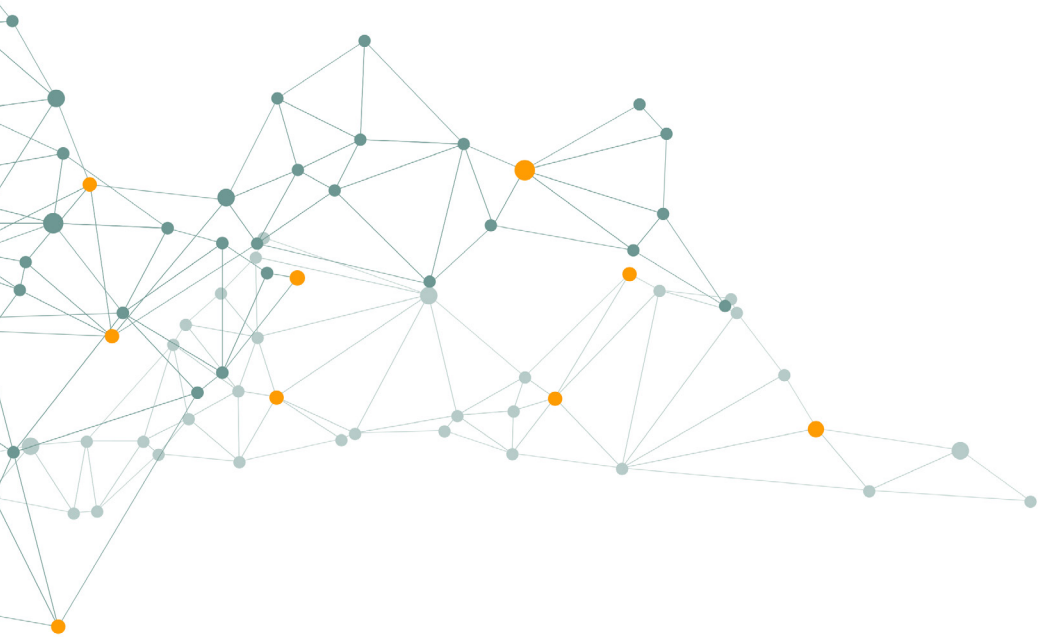
Introduction

This document constitutes the second edition of the CISO Current report and contains data gathered from direct interviews surveying almost 40 cybersecurity executives at leading enterprises from YL Ventures' Venture Advisory Board.

Our distinguished participants responded to a series of questions (see Appendix) to provide YL Ventures' analysts with insights into the cybersecurity market's concerns and opportunities. As the year comes to a close, they were keen to explore the most significant cybersecurity trends of its last quarter as a benchmark for the new year and share their industry predictions for the upcoming decade.

This quarter's interviews and analysis revealed an escalation of CISO preoccupation with digital transformation. As organizations migrate into increasingly complicated and heterogeneous cloud environments, the stakes of their threat landscapes are likewise gaining in complexity and criticality. Large-scale transition and expansion into the cloud, as well as increasing data generation, usage, and analytics, have led to the vast employ of datastores housing growing pools of sensitive data. At the same time, regulations for handling data are broadening and CISOs are growing increasingly concerned with its proper governance. Our research moreover revealed that CISO interest in solutions for identity and access management ("IAM") has also intensified as security advisers search for IAM capabilities that can cater to the cloud.

Already a critical concern among CISOs, cloud environments have further aggravated the human capital gap plaguing the cybersecurity industry as a whole. The market has yet to offer solutions at the rate in which the threat landscape has developed and created more ground for CISOs to address. Executives are currently forced to devote highly valuable and scarce personnel to employ time-consuming solutions manually to address it instead. This emerging reality begs the question: what can the market offer to counter this predicament? Our experts are leaning towards the possibility and promise of automation. YL Ventures intends to keep a close eye on this prospect and how it might be reconciled with the massive cybersecurity implications of cloud adoption.



Leading Cybersecurity Concerns

We initiated the research process for this edition of the CISO Current with an open question about our experts' most pressing ongoing cybersecurity challenges and the strategies they have considered implementing to overcome them. Some further delved into how their concerns impact departmental budgets, and to what extent they foresee today's challenges prevailing in the future. We extracted four overarching concerns that appeared as recurring themes throughout this quarter's research.

Human Capital Shortage and Cybersecurity Operations

In a trend previously discussed in our inaugural report, deficits in human capital and security operations persist and worsen in an increasingly dire trend for the industry. 47%[1] of our respondents listed the human capital shortage and operational gaps as their most pressing concern. They attributed the issue to difficulty in finding the right technological talent for their needs, largely owing to a lack of adequate industry training. It is compounded by the increasing need for employees to operate an ever-growing pool of vendors and tools.

21% of our respondents are certain that the human capital shortage will only intensify in the next five to seven years. They substantiate this prediction on the basis that enrollment in relevant academic fields is too low to produce enough talent to meet existing and anticipated demand. Many also conceded that the accountability and level of responsibility associated with currently open positions often deter the few graduates that do qualify, in a trend that is unlikely to subside in the near future. If attracting and retaining qualified personnel can no longer sustain cybersecurity operations, our experts speculated that reducing the overall need for personnel may assist in alleviating the human capital gap at the core of their operational concerns.

47% of our respondents listed the **human capital shortage and operational gaps** as their most pressing concern.

Largest Budget Allocations

21% Human Capital Shortage

21% GRC & Compliance

16% EDR

Many of our respondents discussed the potential for automation to help replace the need for people in their organizations' increasingly unoccupied roles. This is a particularly suitable solution for repetitive tasks that require smaller amounts analytical effort, such as work traditionally carried out by Tier 1 SOC analysts. However, many are still looking to increase the hiring pool and relayed interest in tapping into new and diverse resources of talent, recruitment, and training alternatives.

Correspondingly, our research uncovered that human capital and training have received significantly increased budgetary shares this quarter. In fact, CISOs are now spending the largest portion of their budgets on human capital after concluding that even the best-of-breed tools do not yet sufficiently address their most pressing cybersecurity issues. This is especially true for newly emerged threats and when CISOs require more customizable and tailored capabilities for their organization's needs. Our analysts are keen to track how this concern will be weighed as the gap abides in the upcoming decade.

[1] Specifically, 26% cited human capital and 29% cited cybersecurity operations as a concern, though a number of the respondents assigned equal weights of importance to both. Our calculations amount to 47% after taking this overlap into account and counting each respondent only once.

Cloud Security

Our respondents cited cloud security-related challenges as their next most significant concern, with 37% specifically listing it among their top priorities. This result directly correlates with the larger trend of digital transformation among enterprises, of which a growing number of organizations, large and small, are taking part. The need to secure cloud environments is only projected to intensify as organizations continue to transition larger amounts of their infrastructure and applications to the cloud and late adopters join the migration procession. This need remains acute at all stages of the process.

Major related challenges cited by our respondents included picking the right tools or partners to support their migration and maintenance of cloud security. Many also discussed the difficulty of scaling their transition without hurting productivity. Notable mentions in this regard included sensitive data migration, encryption and tokenization of data in the cloud, and moving data services to the cloud.

For enterprises with data already in the cloud, securing cloud environments is particularly onerous for those that operate with multi-cloud infrastructure. Participants shared that they were looking to streamline their solutions. Consequently, they are more interested in addressing their cloud concerns through the acquisition of one security solution to cover their multiple environments instead of relying on those furnished by their different cloud providers or by disparate cloud security solutions. Nevertheless, a small number expressed interest in the security products and features of native platforms and remain open-minded to what cloud vendors might offer down the line. They may not have to wait long. Cloud vendors have recently begun to launch multi-cloud management capabilities of their own. While still in their infancy, YL Ventures will be keeping a close watch on this development's potential to progress into native offerings of multi-cloud security tools as well.

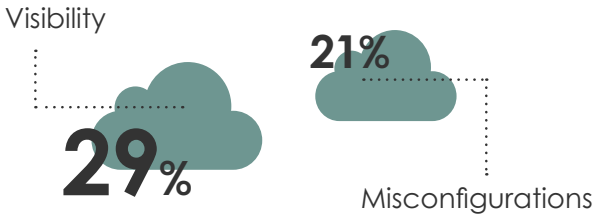
Biggest Cloud Adoption Challenges

Respondents were asked to share the most pressing new risks they must contend with as they increase cloud adoption. Their answers offered a marked change from the responses we received last quarter and excellent insight into how their challenges have evolved.

I. Visibility

Visibility remains a major challenge for our respondents as they migrate to the cloud, though at a significantly higher degree this quarter than in Q3 2019. Many specifically cited issues in visibility related to logging and monitoring and affirmed that their current cloud vendors no longer offer the superior visibility once enjoyed in the past. CISOs today are also concerned with ensuring visibility ahead of moving to the cloud. Solutions using agent deployments that traditionally provided in-depth visibility are growing increasingly obsolete in cloud environments, as the transitory nature of the cloud does not reconcile with the high level of complexity needed to deploy agents on every host and leads to only partial coverage. Many CISOs are troubled by the severe lack of asset awareness organizations suffer on account of obscured visibility. Their concern is compounded by the fact that recent notable breaches specifically occurred in Amazon S3 buckets that were mistakenly thought to be secured or that organizations were simply unaware of. Their outlook on the development of this problem is bleak at best.

Top Cloud Adoption Risks



II. Misconfigurations

Misconfigurations constitute another significantly elevated concern among respondents in comparison to Q3 2019. Many CISOs are acutely suffering from finding and implementing a set of controls for the cloud that function as equivalents to their on-premise counterparts. Moreover, airtight security configurations have become essential to organizational security postures as more infrastructure is moved to the cloud, cloud service providers increase their native offerings, and organizations increase the use of IaaS, SaaS, and PaaS. This was most clearly demonstrated in the recent Capital One data breach, which was a result of a misconfigured web application firewall (WAF). This misconfiguration compromised nearly 140,000 credit card customers and 80,000 bank account numbers, impacting 106 million customers and applicants, and costing Capital One between $100-150 million in 2019[2].

[2] https://www.cnet.com/how-to/capital-one-data-breach-what-you-can-do-now-following-bank-hack/

Privacy, Regulations, and Data Security

Data security and privacy are taking up more mindshare of CISOs and are often tackled under the umbrella of a single task force. As such, it is not surprising that the lines between CISOs and DPOs are growing increasingly obscured. Insofar as data security is concerned, our respondents were most concerned over how to strengthen controls around data lakes and understanding data flows within their organization.

Organizations are dealing with a growing number of blind spots in their efforts to better locate their data in all of its states. This is a cause for significant concern, given that knowing where data is located is a fundamental building block of data security — CISOs naturally cannot secure data they cannot find. Our respondents shared that their need for reinvented solutions in this domain has grown more acute. They qualified this need after sustaining considerable disillusionment with many of the market's current DLP solutions.

High profile fines and class action suits have also brought CISO concerns over data privacy to the fore. Since the GDPR came into force in 2018, a significant number of other national and regional privacy regulations have followed.

Knowing where data is located is a fundamental building block of data security — CISOs naturally cannot secure data they cannot find.

Their enforcement has since significantly matured. Last July, British Airways was fined $240 million (£183.4 million) for a data breach in what is currently the biggest GDPR fine to date[3]. Last quarter, in October, a €14.5 million ($16.04 million) fine was issued to Deutsche Wohnen SE, the highest GDPR fine to be issued in Germany[4]. It followed the UK Court of Appeal's approval of a class action suit against Google for secretly tracking Safari users[5]. With the growing introduction of Data Subject Access Requests (DSAR) proceeding the GDPR, consumer understanding of data privacy has also matured.

Consequently, CISOs are searching for products that can deliver granular consumer data to meet the growing demand from regulators to enable customer DSAR. This poses a difficult challenge, as most organizations lack clear visibility into their dataflows and, due to a lack of available solutions, are forced to manually source these requests on a case-by-case basis.

Our experts anticipate that privacy regulations will remain a primary concern for the next five to seven years. Multinational companies already struggle to manage regulations and privacy efficiently across the diverse territories in which they operate. It is a problem bound to grow as the amount of regulations around privacy and security intensify along with their corresponding enforcement. Our experts predict that states in the U.S. will soon follow in the steps of California's introduction of the California Consumer Privacy Act (CCPA) and introduce their own state-based regulations in the near future. Should these projections materialize, they will directly affect any company that deals with consumer data.

[3] https://techcrunch.com/2019/07/08/uks-ico-fines-british-airways-a-record-183m-over-gdpr-breach-that-leaked-data-from-500000-users/
[4] https://www.dataprotectionreport.com/2019/11/first-multi-million-gdpr-fine-in-germany-e14-5-million-for-not-having-a-proper-data-retention-schedule-in-place/
[5] https://www.ft.com/content/a0a0a1ac-e4ff-11e9-b112-9624ec9edc59

Identity and Access Management

Identity and Access Management (IAM) solutions constitute a growing interest among CISOs. This upsurge occurs against the backdrop of increasingly complex enterprise infrastructures and highly mobile connected devices that transgress the physical perimeter of traditional corporate information security systems. Meanwhile, as environments grow progressively ephemeral due to cloud technology, the escalation of data-driven strategies among enterprises have caused the demand for accessing them by users and applications to skyrocket.

The lack of adequate solutions have prompted CISOs to look inwards for alternative options.

Concerned with access control for both users and applications, CISOs are searching for solutions that promise to address this space. However, while some have found success, a number of our respondents shared their struggle to find solutions that fit their particular use cases—such as managing edge-cases, accounting for frequent role changes, and accommodating the access permissions of cross-departmental projects. Respondents were also concerned with how to reconcile IAM with their business operations so as not to suffer from customer-facing friction. Finally, many found that only point IAM solutions currently receive proper redress by the market, making them far too narrow to address their much wider needs.

The lack of adequate solutions have prompted CISOs to look inwards for alternative options. Some respondents that cited IAM as a major concern have moved to building their organization's IAM capabilities internally, whether on-premise or in the cloud. A number have made special customizations to existing IAM solutions and filled in remaining gaps with supplemental, internally-built solutions.

Some respondents who flagged IAM as a current concern believe it will remain so five to seven years from now. They anticipate growing pains as their data grows increasingly sensitive and broadens in size. Organizations already struggle to map out their data and its flows, process and accommodate the growing number of enterprise applications, and navigate increasingly complicated infrastructure. These difficulties amount to very strained and challenging access management—an issue destined to cause more strain as organizations accumulate more data over the coming years.

AI as a Future Pain Point

The cybersecurity industry has developed at an unbelievable speed as both defenders and attackers race to achieve superior tactics and sophistication. We asked our respondents to share which fields they predict will constitute their biggest pain points in the next five to seven years. In addition to the aforementioned concerns relating to the human capital shortage, developing regulations, and IAM, respondents notably flagged AI. Over a quarter of respondents shared their fear of future AI-generated and targeted attacks. They are specifically concerned with the growing sophistication of artificial neural networks that are already enabling the creation and production of attacks, including audio and video deepfakes.

The DeepFake Detection Challenge (DFDC), conceived by major corporations like Facebook, Microsoft, and Amazon, as well as Twitter's introduction of its new policy to help fight deepfakes, are some indications of just how top of mind AI threats have become for prominent technological enterprises and other leading industry organizations. Deepfakes have a tremendous spectrum of implications, particularly on the banking industry, media industry, and on social networks. Doctored video and audio have demonstrably serious ramifications; the lack of controls in place to counter or regulate them leave room for considerable reputation and financial consequences. Our experts share that deepfake anxieties are no longer grounded in speculation or forward thinking—bank account openings, Know Your Client (KYC) processes, money transfers, and account changes are increasingly being carried out through video authentication and executive fraud is increasingly taking place using forged audio.

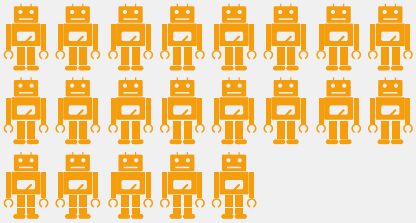
Moreover, our experts are concerned by how the increased use of machine learning and artificial intelligence within their enterprises will eventually turn AI models into targets for cybersecurity attacks. Our respondents have given this more attention in light of the recent bypass of Cylance's AI-based antivirus detection algorithm, achieved by leveraging a bias in the AI model. Some speculate that the bypass foreshadows imminent attacks on the ever-growing number of AI models servicing enterprises across all industry verticals. AI continues to make significant gains in the private sector and it is imperative to maintain the integrity of its models; our experts are concerned with how their enterprises can secure their AI algorithms against theft and tampering as they become operational staples.

IR, SOAR, and Detection & Response

We asked our respondents to discuss the most recent additions to their cybersecurity budgets and impart what items received an increased share. While a sensitive topic by nature, our experts were quite candid in their responses and provided illuminating insights into their organization's fiscal priorities. In addition to increased budgets pertaining human capital, respondents also mentioned incident response, SOAR (Security Orchestration, Automation and Response), detection and response.

Increased Budget Allocations

21% IR/SOAR/MDR



16% Human Capital Shortage

Many CISOs concede that their organizations will never achieve total end-to-end security and that no organization can feasibly block every attack launched against their systems. For this reason, an increasing number of organizations are moving beyond a singular focus on attack prevention and onto emphasizing detection and response. Incident response, SOAR, and detection and response have consequently been earmarked as more prominent cybersecurity budget items. Our respondents are determined to minimize the time taken to deal with vulnerabilities and breaches, improve their detection capabilities, and issue faster remediation. Many are open to, or already outsourcing, such capabilities to meet this need.

For those looking to keep these capabilities internal, this segment of the industry is a perfect candidate for automation solutions, as automating incident response can leave valuable security practitioners available for tasks that require a greater deal of in-depth thinking. This segment has also enjoyed a recent spike in innovation. While still unable to remediate on all fronts, existing tools offer an excellent next step towards that goal and our experts anticipate that cloud providers are next in line to offer a product that can tackle this issue.

Final Observations

Cloud ubiquity among enterprises has brought forward a variety of old and new CISO concerns. It has generated heightened interest in cloud visibility and misconfigurations as well as increased challenges around specific use cases that include digital transformation and multi-cloud security.

Moreover, this increasingly deployed technology has reprioritized identity and access management among enterprise security teams and executives. IAM, a well-established concern in traditional on-premise environments, has recently reemerged as a challenge of unprecedented scope in light of large scale and ongoing cloud migration. Cloud technology is also changing how organizations store, transfer, process, and analyze their data while their very relationships with data change in their pursuit of data-driven strategies. Security teams must consequently contend with increasing amounts of sensitive data while concurrently managing a larger pool of BI and analytics tools and ensuring overall compliance with maturing privacy mandates.

The shortage of skilled human capital in cybersecurity teams only compounds all of these aforementioned concerns. The market does not sufficiently meet the needs of security teams, thus necessitating their manual performance of time-consuming tasks instead. Their unavailability to carry out mitigating measures against the mounting threat landscape only increases the already critical demand for skilled employees. Ultimately, until automation can help fill this widening gap, CISOs will resort to enlisting the service of creative solutions that can help them streamline the security of their ever-growing cloud environments.

Outreach and Contact Information

This report was compiled with Israeli cybersecurity entrepreneurs in mind. If you are an Israeli-based start-up looking for guidance for seed-stage funding, we invite you to contact:

YL Ventures Partner & Head of Israel Office
Ofer Schreiber **ofer@ylventures.com**

We would like to sincerely thank all of the CISOs that participated in this report. If you are an industry expert and would like to be interviewed for the next edition of the CISO Current, please contact:

YL Ventures Partner
John Brennan **john@ylventures.com**

We also invite any questions relating to this report to be directed to:

YL Ventures Analyst
Naama Ben Dov **naama@ylventures.com**

Appendix

Interview and Survey Questions

- Name your 3 biggest current cybersecurity challenges and describe your plan to resolve them.
- Share 2-3 fields that you predict will be huge pain points 5-7 years from now.
- Share new risks you find yourself facing as you increase cloud adoption.
- What are recent additions to your cybersecurity budget?
- What items have received an increased share of your cybersecurity budget?
- What cybersecurity products and technologies have you built internally due to a lack of existing viable market solutions?