YL VENTURES
The CISO Current

The CISO Current Report

Q1, 2020

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 $270 million and exclusively invests in cybersecurity.

YL Ventures 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 fund's focused strategy allows it to conduct rapid and efficient evaluations for early stage entrepreneurs and guide founders through their ideation processes pre-investment. The fund is also dedicated to providing unmatched hands-on value-add support for each of its portfolio companies, both strategically and tactically, across multiple functions post-investment.

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 composed of over 80 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

satori
Secure Data Access Cloud
www.satoricyber.com

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

orca security
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

RIDE VISION
Predictive Vision for Motorcycles
www.ride.vision

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 third 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.

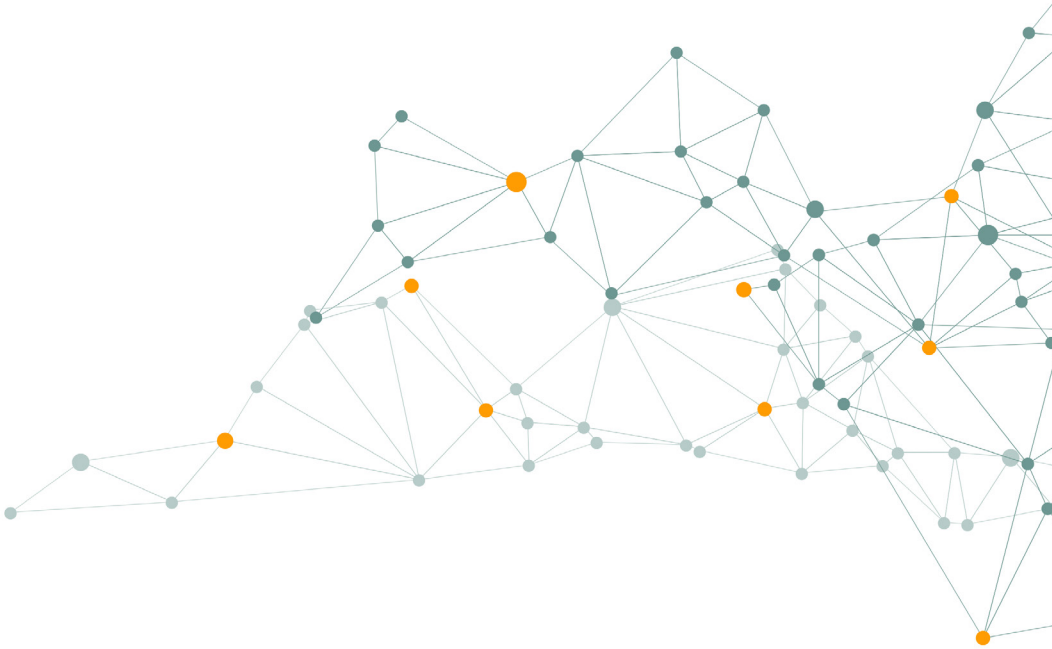
Surveys were conducted through short-form questionnaires and longer-form interviews. In order to obtain the most candid data possible, and with respect to the sensitive nature of some of the information shared, we have anonymized the names of our respondents and their associated organizations.

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. The impetus for this edition was to thoroughly explore a select trending topic in the cybersecurity space. With the support of YL Ventures' CISO-in-Residence, our research team selected "DevSecOps" as the inaugural subject for this approach. This is a space in cybersecurity that still begs cohesive definition and investigation with regards to its market potential.

Nonetheless, as the COVID-19 outbeak transgressed into a global pandemic midway through Q1 2020, it became evident that this report would be incomplete without addressing the significant changes that have accompanied its effect on the market and industry. YL Ventures' specific intention in dedicating a section of the CISO Current to COVID-19 is to shine a light on how cybersecurity startups can most successfully forge ahead and how CISOs across many verticals are coping with these new changes.

Just as our unique position in the cybersecurity ecosystem allows us to bridge communication between vendors and customers on the market's potential, so too should this report provide guidance on how to move forward in these difficult and confusing times. To this end, we consulted with the broader executive cybersecurity community and customers in our network to share their insights and perspectives. The experts we consulted were particularly adamant that vendor engagement with CISOs will need to adapt to the new realities laid out by COVID-19.

In order to disseminate the DecSecOps findings already assembled by our team, as well as remain true to our desire to publish top-of-mind data and information for our readers, we adjusted ourselves accordingly and opted to split this quarter's CISO Current report into two sections. The first will discuss our DevSecOps findings and the latter section will discuss what our experts have shared about the emerging challenges they face as a result of the pandemic. To this end, it will provide guidance for early-stage cybersecurity entrepreneurs and vendors on how to best maintain meaningful relationships within the cybersecurity ecosystem and support enterprise security in today's dramatically changing landscape.



DevSecOps

DevOps and agile development produce applications faster than traditional software development methods. However, the "need for speed" at the core of DevOps, as well as some of the methodologies used to manage it, have exposed organizations to a great deal more risk than the expediency it achieves may be worth.

While efforts to "Shift Left", or introduce security earlier into code development, are hardly new to the industry, the concerted effort to consciously implement "security" in DevOps is a more recent addition to cybersecurity discourse. "DevSecOps", the marketing term coined to denote this methodology, remains controversial to the majority of experts we consulted. By the nature of their security executive ethos, many consider it a buzzword for something they have been angling towards in their organizations for quite some time. Nonetheless, many appreciate the market potential of DevOps security solutions and, to that end, shared the quantitative and qualitative data that follows in this report.

In the realm of providing security for code development, our experts' most prevalent concerns pertain to data leaks, code integrity, releasing insecure code and the suitability of existing solutions to modern code development environments. In their efforts to address these concerns, our experts foremostly face the challenge of strained collaboration between security and development teams, finding and implementing the right processes to attain maximized security and obtaining buy-in from DevOps and security practitioners.

Many appreciate the market potential of DevOps security solutions and, to that end, shared the quantitative and qualitative data that follows for this report.

Ultimately, challenges pertaining to processes and management, rather than delivering improved technology, remain the biggest obstacle to secure code development—an issue that is only exacerbated by modern development methods and environments.

Code Development Process Concerns

Data Leaks

31% of the experts we consulted cited data leaks as their primary code development process concern. While some were worried about the involuntary release of internal data, most were more preoccupied with data leaks in externally-facing products and accidentally leaking sensitive data of customers, such as personally identifiable information (PII).

Our experts warn that back office operation code is more exposed to data leaks, given that it tends to follow less security processes. Internal business applications may present a greater risk compared with customer-facing applications, as they are not often required to abide by customer security stipulations, contracts and commitments. Our experts explain that certain processes, such as running CRM and ERP systems do not require contractual obligations to customers pertaining to security. This in turn exposes organizations to yet another layer of risk that is often ignored.

One expert we consulted is working with a startup curbing data leaks by scanning their code and running unit and integration tests to discover the source of its leaks. They also mentioned mitigation efforts by way of separating between developers' private and non-private code. Experts mentioned their use of static code analysis tools (SAST) as a key part of their pipeline to shore up their code development security. However, they conceded that this solution fails to offer full coverage. Therefore, in order to catch what is missed, the enterprise additionally runs quarterly penetration tests on their own services with a primary focus on systemic issues, rather than individual incidents.

Suitability to Modern Development Methods and Environments

28% of respondents are concerned with the dissonance between existing security tools and practices and the requirements and realities mandated by increasingly modern development practices. Our experts are quite actively looking for solutions to mitigate this risk, especially as organizations increasingly migrate towards cloud-native environments and use modern technologies such as Kubernetes, microservices and CI/CD pipelines.

Some object to the use of open source security tools by development teams. While many exist, they involve too much maintenance and overhead to properly address issues in a timely and efficient manner. Other executives are finding more optimal open source solutions in the latest generation of products.

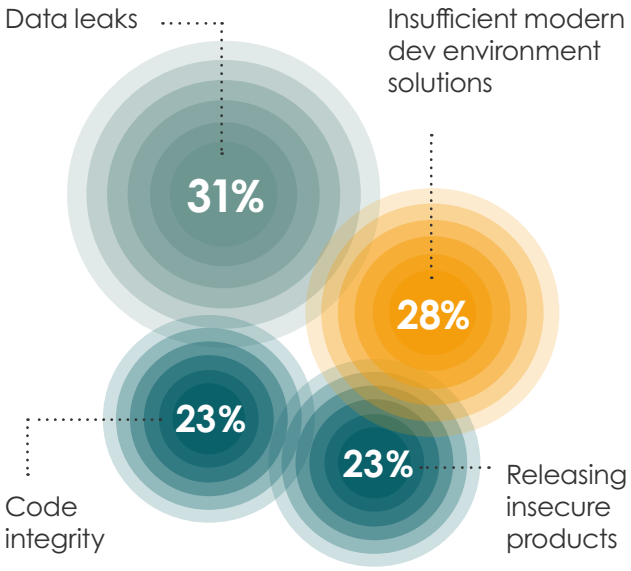
However, nearly all of our respondents struggle significantly in both sourcing and implementing the right static and dynamic application security testing (DAST) tools for their increasingly agile development environments. Specifically, most SAST and DAST solutions take too long to run, effectively rendering the expediency of DevOps and agile development moot. Secondarily, our experts complained that their solutions produced too many false positives, requiring security analysts to dedicate an enormous amount of time to review results that only produce a marginal number of actionable items.

This problem is further exacerbated when the results containing false positives are shared with developers. This leads to issues in credibility and is a point of strain between developers and security teams. Moreover, many solutions require compulsory intervention on the part of developers, despite their "developer-unfriendly" design. This adds a layer of inefficiency and complexity that ultimately slows down both development and security processes.

Insofar as runtime application self-protection (RASP) and interactive application security testing (IAST) are concerned, our respondents were quite candid that they have not yet included any in their stacks. Their hesitation largely lies in their requirement to be deployed by engineering teams that are, by and large, unmotivated to do so.

Some of the experts we consulted with are interested in exploring open source or cloud native tools while increasingly involving those with actual roles in the application development process. However, this requires executives to direct a significant amount of resources to training in areas such as OWASP and other various vulnerabilities that applications entail.

Top Security Concerns: Code Development



Code Integrity and Releasing Insecure Products

Code integrity and releasing insecure products respectively were listed by 23% of our surveyors as a primary concern. The CISOs who flagged code integrity were focused on releasing high quality code devoid of bugs, corruption and tampering. They achieve this by attaining high code coverage through unit testing and integration testing. As expected, the consulted executives were more concerned with the code integrity of their internal applications than they were about externally-facing applications. However, CISOs were also more concerned about releasing insecure code vulnerable to exploitation in externally-facing products, rather than applications built for internal use.

This is a telling juxtaposition. The combination of these findings indicate a slight preference towards the security of code built for externally-facing products over code written for internal business applications. Nonetheless, CISOs still primarily strive for applications to run smoothly and correctly. This can largely be explained by the fact that customer-facing applications are open to the internet at large, thereby heightening their organization's visibility and vulnerability to external attackers. On the other hand, it takes significantly more effort to penetrate an organization through an internal application.

By and large, these findings echo the aforementioned point that certain internal applications are less secure as they are not subject to contractual obligations by customers pertaining to security.

Challenges in Implementing DevSecOps

Collaboration Between Security, Development & Operations Teams

The cybersecurity experts we consulted with acknowledge that different team backgrounds and priorities can pose significant points of friction. However to this end, they recommend using the same tools where possible. They moreover recommend increasing their security teams' understanding of software development tools and of how code gets deployed as well as regularly touching base on APIs.

Given that engineers are increasingly responsible for adopting security measures, our experts are adamant that security personnel must develop familiarity with engineering practices in turn.

Given that engineers are increasingly responsible for adopting security measures, our experts are adamant that security personnel must develop familiarity with engineering practices in turn. This would allow security teams to operate within their practices as well and foster better inter-departmental understanding. Nonetheless, the cyber executives we consulted maintain that training developers on secure coding is still necessary and carries more weight in achieving fundamental hygiene more quickly. Some have attempted to use incentivizing programs and train developers using targeted platforms with relative success. They also recommend utilizing libraries or frameworks with security built in for them.

Moreover, many of our experts insist that a wider cultural shift is necessary for more lasting changes. Developers are incentivized to generate code and features of high quality, performance and efficiency, but are not security oriented by nature. By consequence, security is hardly top of mind for the average engineer as they carry out their daily tasks. This is largely owed to the general lack of meaningful security coursework or integration of security training in their formative university education or professional training.

Our advisors argue that it is important to instil a new security mindset early in these programs with a specific focus on critical thinking around how code creations can break and the risks involved in the build stage. This is largely informed by the particular pushback against their efforts to introduce such mindsets among existing workforces, especially among veteran engineers that have been with their organizations the longest. By their account, it is very difficult to encourage a shift in culture or mentality among veterans or facilitate knowledge transfer from organizational newcomers, given their professional pride and resistance to change. Our research made clear that this issue pervades all verticals and is not industry-specific.

41%

Of respondents are concerned about collaboration between security and DevOps

Finding and Implementing the Right Processes

A substantial amount of our respondents, 38%, have faced great difficulty in implementing the right processes to secure their code development. The largest challenge lies in scalability and keeping security hygiene without losing efficiency. Security resources are failing to grow at the same pace as development resources and lines of code. By consequence, a static number of security personnel find themselves tasked with overseeing larger and larger amounts of code.

38%

have faced great difficulty in implementing the right processes to secure their code development.

This is further catalyzed by the development of internal applications, given how difficult it can be to track their code. These internal efforts are supported and encouraged by development practices that allow non-tech users to create applications, especially for tools built into platforms like G-Suite and Salesforce. They are also growing more frequent as more employees self-teach to code. Despite these difficulties, security teams are pressured to cause as little friction as possible in the production of such applications. Our experts claim that the "process problem" stems from this prioritization of features development and productivity over security features.

Our advisors argue that security teams ought to be involved as early as possible in the SDLC. In an ideal framework, this would entail security at the very beginning of code building, working on its technical specifications and gathering product requirements to inform how it will take form. Such a process would enable teams moving beyond the build stage to have already integrated security from an architecture perspective.

Once again, the experts we consulted with suggested encouraging security teams to both understand and use the same tools and practices as their engineering counterparts. For instance, if engineers deploy IaaS using TerraForm or CloudFormation, then security teams ought to know their native security functionalities as well. This approach would create a cross-organizational standard and build a culture of security around running processes and deploying software.

One executive proposed building security testing integrally into the code development process in the same manner as quality or performance tests are currently integrated. The caveat, however, is that it can only succeed if it is invisible, lest it hinder the overall process. Insisting that the ultimate aim is to make it part of the process, our experts shared how they must constantly consider balancing speed of development with security quality.

Another executive is working to alleviate these issues by inserting themself into governance by flagging the exact point of security impact across their organization's decision-making processes. They also proposed using tools to facilitate visibility and transparency in communicating risk, though they added that they must have bearing on the CTO and VP Engineering of an organization.

Buy-in from Development, Operations and Security

18% of our respondents cited security buy-in from DevOps and from Security as one of their biggest obstacles to adopting DevSecOps. The need for expediency once again served to explain this area of organizational contention. Cybersecurity experts find themselves walking a fine line between business objectives and security and are careful to avoid causing operational slowdowns.

18%

cited security buy-in from DevOps and Security as one of their biggest obstacles to adopting DevSecOps.

To overcome this hurdle, our experts suggest encouraging developer ownership over everything they build, starting with accountability for security. This approach is meant to help developers internalize the risks of insecure code in order to incentivize them to create secure code from the onset. To this end, self-service remediation is heavily recommended. According to some of our experts, developers must have the control to mitigate their own risks. Moreover, improving security approachability is a secondary key to helping this collaboration succeed. Developers cannot fear reasonable risk-taking and security teams must avoid negative reinforcement when mistakes are made.

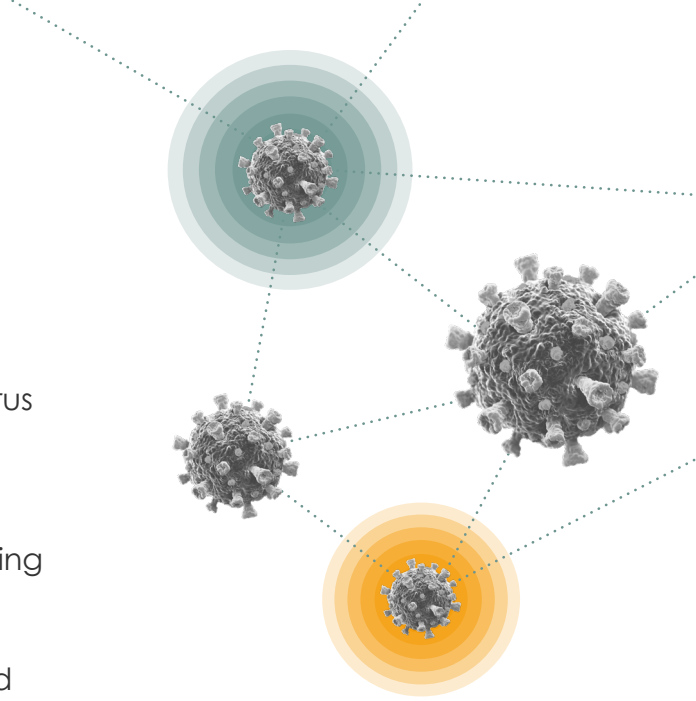
This can also be further encouraged by incorporating security training into their process with a system of positive reinforcements for completing a course or established markers of success. Such courses of action may engage them throughout the entire process, providing education and validation that changes are made without conflict.

Final Observations

In the realm of providing security for code development, our experts' most prevalent concerns pertain to data leaks, code integrity, releasing insecure code and the suitability of existing solutions to modern code development environments. In their efforts to address these concerns, our experts foremostly face the challenge of strained collaboration between security and development teams, finding and implementing the right processes to attain maximized security and obtaining buy-in from DevOps and security practitioners.

Ultimately, challenges pertaining to processes and management, rather than delivering improved technology, remain the biggest obstacle to secure code development—an issue that is only exacerbated by modern development methods and environments.

The Impact of COVID-19



At the time of the writing of this report, the coronavirus strain coined COVID-19 continues to spread unchecked across the world. To date, scientists have yet to find an effective treatment or cure. World-wide, countries are in various stages of instituting unprecedented nation-wide quarantines with tremendous sociological and economic impacts. The market has taken a series of dives as a result and has remained in flux with devastating economic results.

Those still employed are encouraged to work from home unless their specific position requires otherwise. Such decrees are part of larger "shelter-in-place" mandated by local and federal authorities with various degrees of legal backing and enforcement. It is unclear when such measures can be expected to be lifted.

Historically, times of trouble lead to a rise in cybercrime. Reported phishing and fraud attacks have sharply risen since this outbreak began to spiral in addition to attacks on health organizations. Moreover, corporate VPNs open up a myriad of security vulnerabilities for enterprises that are certainly not primed for this unprecedented influx of workers logging in from home. Digital transformation laggards are feeling particular strain as they scramble to migrate to the cloud and support remote workforces. All of these unfortunate vulnerabilities necessitate greater enterprise cybersecurity protection and will likely be top of mind for industry stakeholders as a result.

Like all other verticals, even an ecosystem as robust as cybersecurity has felt the strain of COVID-19's economic effects. The industry may need to anticipate a short-term sales drop as organizational austerity measures kick in among their customer bases. However, the unfortunate realities of cybercrime rates in times of economic crisis, as well as the new vulnerabilities presented in the vast migration of remote workers, will likely reverse any such drops relatively quickly.

Our findings indicate that CISOs are mostly concerned with issues pertaining to remote work, both in terms of securing it and operationalizing it. The professional and personal strain brought about by these rapid and dramatic changes have left them with far less time and resources to spend on vendors.

They are moreover contending with budget constraints that necessitate expense cuts. Vendors cannot operate in the same manner as they did before this crisis; They must garner both empathy and patience towards customers and leads, and find ways to translate this into professional practice as they continue operating.

Additionally, CISOs advised startups to carry out goodwill gestures for the industry and their local communities, as well as nurture their existing relationships, rather than focus on building new customer relationships. They also adamantly recommend that vendors reduce cold email frequency, embrace brevity and avoid using COVID-19 in sales pitches.

New Challenges

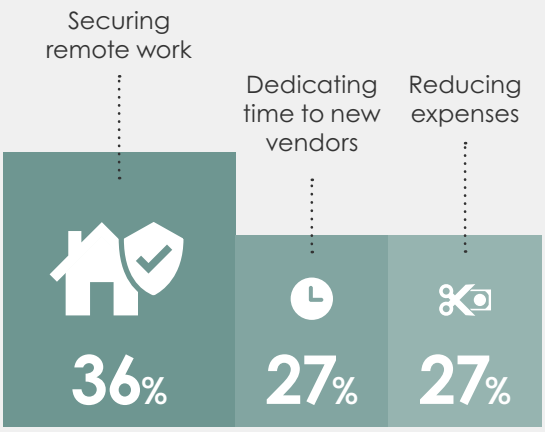
Establishing Fully Remote Workforces in Limited Timeframes

CISOs are in the process of adjusting to unprecedented operational changes as entire organizations transition into virtual companies over the course of days. The scale and speed required in carrying out such changes securely requires an incredible amount of streamlining and single-minded dedication. 36% of our experts warn securing and managing remote workers is their top priority and that now is not the time to present CISOs with anything other than solutions to directly help these processes, ideally in a "plug and play" type format. Expediency and simplicity have never been more crucial, and anything that does not serve these purposes will be disregarded as "noise".

Dedicating Time and Effort to Explore New Vendors

As previously mentioned CISOs are currently under immense strain to support organizational pandemic programs. Entrepreneurs are encouraged by our advisors to consider how else this transition will affect vendor trials and diligencing. From an organizational level, it will take time for enterprises to gain their bearings in an entirely remote structure. They can expect non-critical missions to effectively halt or grind to a near halt as a result. 27% of our experts explain that innovating around new security and privacy technologies outside of directly servicing these goals simply cannot abide in these new timeframes. Personal considerations of the cyber executives vendors aim to target must also be considered, especially those with dependents placed fully under their care.

New Customer Challenges



Organization-Wide Austerity Measures

Cybersecurity executives do not work in a vacuum. They are crucial entities in a larger executive network with organizational budgetary constraints. As the economy fluctuates, cuts are taking place across the board of most organizations. Most enterprises are focused on remaining afloat and maintaining their payroll in a timely manner. While many enterprises have prioritized cybersecurity in recent years, the domain has not yet developed immunity to the financial realities of the times, says 27% of our cybersecurity executives. Therefore, in addition to the time and mental bandwidth constraints CISOs contend with today, cybersecurity executives must also scramble to work within narrower budgetary margins as well.

How Entrepreneurs Should Proceed

Avoid Alarmist Pitches

Our experts were firm that there is a fine line between genuine messaging and exploitation, and crossing it will be detrimental to a company's brand. Messaging ought to be geared towards impacting an enterprise's bottom line or community, rather than attempting to fearmonger or stoke panic over a situation already causing CISOs enough anxiety. This is still true for solutions whose value fits well with the current narrative. 23% of our experts counsel that it is still best to focus on value and let customers draw their own conclusions about why a particular approach may be considerably more important in the given situation. They also wished to make clear that there are many lines of communications between CISOs, which is a tight knit community. Cybersecurity executives feel quite unanimously about the marketing frenzy and, according to our sources, are compiling a "black list" of vendors guilty of using this tactic.

Make Goodwill Gestures

Profiteering off of a world-wide tragedy will do vendors little service in the eyes of prospective customers. However, our experts were quick to point out that the situation still presents ample opportunity to stand out against the competition and build goodwill. 41% of the CISOs we consulted with praised technology companies using their services to help other businesses and advised entrepreneurs to follow in their lead instead. Public statements are an excellent start, especially when they are community-minded and offer value. Consider producing webinars or other types of free content to share useful information. This is also an excellent time to consider revising payment methods by instituting deferred payment options to accommodate new budgetary constraints. Vendors are also strongly advised to consider supporting local clinics or emergency organizations pro-bono or with free tools. Moreover, companies should also consider non-technological ways to give back to the community, whether through fundraisers or assisting the more vulnerable.

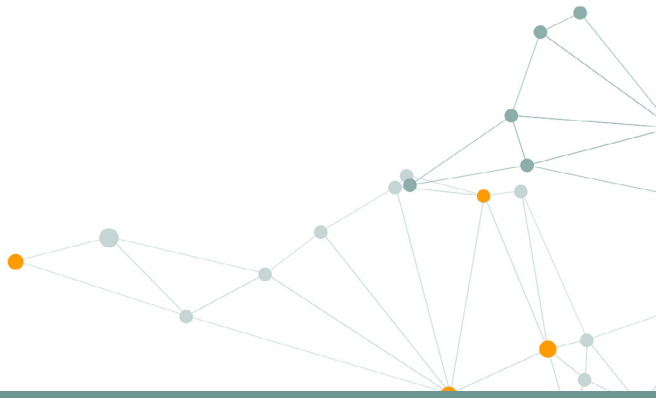
Reduce Email Frequency

Our experts have made their vendor fatigue quite clear over the last two editions of the CISO Current. The current strain they face in shoring up their organization's remote capabilities only underscore this point. CISOs are simply in no position to manage cold calls as they race to support enterprise-wide workforces and have ruled them entirely out of their equation for now. 41% advise entrepreneurs to reduce their outreach or, at the very least, directly ask when a good time to be in touch would be instead.

Nurture Existing Relationships

While this may not be an optimal time to engage new customers, our advisors encourage entrepreneurs to maintain existing relationships and leverage them when appropriate. To the first point, 23% of our experts advise holding smaller and more frequent checkpoints with customers, especially new ones who are still onboarding products. This is an optimal time to check how you might better serve them and be a point of reassurance in this time of crisis. It is especially important for a vendor's tech support to be available and accessible at this time.

Insofar as our CISOs council vendors to leverage new relationships, this may be an optimal time to discover what customers would like to see integrated into the products they are using. With an eye on the end of the crisis, vendors should ask their customers to be candid about how they expect the market to emerge from this crisis and how they can design the best solutions for this possibility. Entrepreneurs should also consider discussing their customers' overall experiences throughout this time. Ask them what they've learned so far that has shocked them. This information can be vital in helping build more robust platforms. Another expert advised entrepreneurs to bring value to an existing relationship by introducing them to other customers in their situations as a mutually beneficial learning opportunity.



Final Observations

As both enterprises and startups cope with the effects of the COVID-19 outbreak, communication between cybersecurity executives and vendors is absolutely paramount to maintain a safe and productive market. Though difficult times may lie ahead, entrepreneurs must note that slower sales are no reason to remain idle. In fact, now is the perfect time to focus on R&D in order to build the best product possible to release once the market recovers. It may be also a good time to redirect sales teams to customer success. Given that most vendors may have to contend with a long period of slow sales or closed doors, making use of this time internally is absolutely imperative. The way that vendors conduct themselves now will cement their reputations long after this crisis has passed. Therefore, in addition to building the best cybersecurity startup possible, entrepreneurs must remember to serve the wider security community positively.

Moreover, this is precisely when entrepreneurs must make the most of their existing relationships and forge ahead in a community-minded manner. To that end, their investors are excellent resources to help organize for what's to come, whether it's by helping reorganize budgets or injecting necessary capital where it is needed most. True value-add investors may even have an entire multidisciplinary staff on hand to support portfolio companies while they regain their footing.

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 Associate
Naama Ben Dov **naama@ylventures.com**

Appendix

DevSecOps Survey Questions

- What are your biggest cybersecurity concerns regarding your code development process and its impact on the company product\service?
- What are your biggest cybersecurity concerns regarding your code development process and its impact on enterprise operations?
- What application security testing tools are you currently using? (e.g. SAST, DAST, RASP?)
- Have you implemented devops?
- Have you implemented devsecops?
- What are your biggest challenges in implementing DevSecOps?
- Who is the key stakeholder for DevSecOps?
- Is DevSecOps a buzzword?

DevSecOps Interview Questions

- What are your biggest cybersecurity concerns regarding your code development process and its potential impact on your company's product(s)/service(s)? How are you mitigating those concerns?
- What are your biggest cybersecurity concerns regarding your code development process and its impact on enterprise operations, and how are you mitigating those concerns?
- What application security testing tools are you currently using? (e.g. SAST, DAST, RASP?)
- Where in your SDLC do you implement security protocols?
- Have you implemented devops?
- Have you implemented devsecops?
- If not, are you planning to implement DevSecOps?
- If so, what are your biggest challenges in implementing DevSecOps?
- Who is the key stakeholder for devsecops?
- Does your organization have a dedicated budget line for DevSecOps?
- What part of devsecops is innovative, and what part of it is just collaborating between infrastructure and security?
- Is devsecops a buzzword?

COVID-19 Interview Questions

- What advice would you give to cybersecurity startups about customer engagement with their existing pipeline and potential new customers?
- What is the most productive course of action for cybersecurity startups in the given situation?