CONTRAST SECURITY

APPSEC FOR THE NEWLY HIRED CISO/CSO

Recommendations on How to Assess Application Security in the First 100 Days

INTRODUCTION

Newly hired chief information security officers (CISOs) or chief security officers (CSOs) are tasked with leading an increasingly critical function. They must protect an increasingly distributed infrastructure from a long list of adversaries with malicious intent who use progressively advanced tactics. Digital transformation increases the importance of application development to many companies' success, and this should move application security (AppSec) up on CISOs' priority list.

This eBook explores the first 100 days of the new CISO/CSO's tenure specifically from the perspective of AppSec. Not too long ago, AppSec would have been a secondary priority that may have been barely mentioned in the early stages of a new leader's tenure. In the current environment, however, AppSec must receive significant attention from day one.

"THOSE WHO APPROACH THE ROLE WITH A STRONG PLAN FOR THE FIRST 100 DAYS ARE LIKELY TO ENJOY SUCCESS."[1]

"THE REALITY IS THAT THE FUNCTION OF A SUCCESSFUL CISO/CSO SHIFTS FROM THAT OF A DELIVERY EXECUTIVE TO BUSINESS ENABLER."[2]

[1] Susan Moore, "Your First 100 Days as a New Chief Information Security Officer," Gartner, September 1, 2016.
[2] Patrick Spencer, "8 Strategic Priorities for a New CISO," The CISO Collective, June 14, 2018.

CONTENTS

30-, 60-, AND 100-DAY PRIORITIES

By Day 30:

- Meet with people across all departments and job levels to understand what makes the company tick
- Meet with every executive and leaders of key stakeholder teams to understand the organization and its infrastructure
- Ensure there is an up-to-date application inventory; if not, start planning for one
- Understand what cybersecurity and AppSec metrics are being captured and devise a plan for expanding and improving measurements

By Day 60:

- Understand what cybersecurity and AppSec
- Perform a gap analysis of processes and procedures for AppSec; build a roadmap to address any needs
- Conduct a Software Assurance Maturity Model (SAMM) assessment to determine current maturity and set the next several phases of goals and measure via the dashboard
- Work on a resourcing plan and determine what software security services are needed to meet application security (AppSec) goals

By Day 100:

- Rank each application according to risk to provide a priority list to focus AppSec resources
- Conduct an awareness campaign so that teams know they can reach out for help with AppSec problems
- Develop an AppSec roadmap and a communications plan for rollout
- Build relationships with other CISOs to help learn from each other's experiences

01

GETTING THE LAY OF THE LAND

If a newly hired CISO/CSO is promoted to the role from within, she or he has the advantage of understanding the organization, but may need to be deliberate about acclimating to the role. For external hires who assume the position, getting one's bearings can involve a surprisingly complex learning curve. Even those who have years of experience in the CISO/CSO role at other organizations must come to a deep understanding of the new company—its culture, its traditions, the lingo and acronyms that are used internally, and formal and informal ways that things get done. As Samuel Liles puts it, "A new CISO should be getting the *ground truth* on what the current environment of the organization looks like."[3] These "soft" attributes inherent to the firm are critical to understand in the first 30 days.

It is also crucial to gain a detailed understanding of the organization's IT infrastructure, its risk profile, competitive landscape, and digital priorities. Part of this investigation is to determine what is currently being measured from a cybersecurity and AppSec perspective—and what further measurements could be gleaned given the current infrastructure.

Part of the challenge facing a new CISO/CSO is that the organization cannot be put on pause for a month or two while the new security leader conducts an investigation and maps out a strategy. "As a new CISO you are bombarded with activities and initiatives that vie for your limited time and attention," says Sean Walls, vice

[3] Samuel Liles, "New CISO? Get Your First 90 Days Action Items Here," Personal Blog, August 16, 2016.

"TO MAXIMIZE YOUR CHANCE OF SUCCESS, IT IS IMPERATIVE THAT YOU UNDERSTAND THE BUSINESS, DEVELOP RELATIONSHIPS WITH KEY INFLUENCERS AND DECISION-MAKERS, AND IDENTIFY YOUR COMPANY'S MOST VALUABLE ASSETS."[4]

president and CISO of Visionworks of America. "But to maximize your chance of success, it is imperative that you focus first on understanding the business."[5]

GATHERING INSIGHTS ACROSS THE ORGANIZATION

To gain this information, the new CISO/CSO must go to a variety of sources. It would be a mistake to rely on just a few people—perhaps peer executives or direct reports of the CISO/CSO—to gain an understanding of these things, as this could result in a skewed perception. Instead, it is important to understand both the official view from executives and the experience of middle managers and frontline workers—on the security team and across the business—who know more about how things work in practice. As Rohan Amin, a CIO at JPMorgan Chase, asserts, "If you spend time only in security land, you really don't understand the complexities the builders go through to deliver."[6]

From an AppSec perspective, this means being deliberate about connecting with teams that rely on applications to be successful. CISOs/CSOs should connect with both department heads and select end-users who actually operate different pieces of software for the company. Insight into their everyday challenges will help the CISO/CSO to build effective AppSec solutions that propel the business rather than impede it.

[4] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.

[5] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.

[6] Rohan Amin, CIO, Consumer & Community Banking, JPMorgan Chase, quoted in "Protecting the Business: Views from the CIO's and CISO's Offices," McKinsey, March 2020.

MAPPING THE APPLICATION LANDSCAPE

Understanding what applications are out there, what they are used for, and how important they are is critical in the first 30 days. This includes not only homegrown and out-of-the-box applications managed by IT, but also business-managed applications that often reside in public clouds. With a little research, it would not be unusual for a CISO/CSO to discover applications in use that the CIO was unaware of—but should be secured. Shadow IT, which includes applications developed by individual departments and groups, comprises upwards of 50% of an organization's IT spend today.[7] And this should be alarming, with Gartner predicting that Shadow IT will be the cause of one in three security breaches this year.[8]

"DON'T START TO MAKE PLANS UNTIL AFTER YOU LISTEN FOR A LONG TIME."[9]

Ideally, the organization will already have a detailed application inventory that is up to date and regularly maintained. This repository should give the CISO/CSO the information needed to map the entire application attack surface throughout the software development life cycle (SDLC). If such an information source does not exist, the CISO/CSO should find team members who can assemble one quickly and set it up in such a way that it can be maintained easily.

This step is especially important given the turmoil caused by COVID-19, when digital initiatives may need to be delivered quickly. One survey conducted after the crisis was underway finds that 64% of organizations plan to increase their adoption of Agile IT and DevOps practices during the pandemic.[10]

[7] Peter Bendor-Samuel, "How to Eliminate Enterprise Shadow IT," CIO.com, April 11, 2017.
[8] Kasey Panetta, "Gartner's Top 10 Security Predictions," Gartner, June 15, 2016.
[9] Private correspondence with Brian Glas, longtime cybersecurity leader and assistant professor of Computer Science at Union University.
[10] "How IT Operations Leaders Can Not Only Survive But Thrive During The Great Lockdown," OpsRamp, accessed May 6, 2020.

ASSESSING THE APPSEC PROGRAM

Some CISOs/CSOs will find relatively mature AppSec programs in place when they arrive, but many will find legacy approaches to AppSec that create delays and other headaches for developers while providing inadequate security. Here are some questions that an incoming CISO/CSO could ask of the development and DevOps security teams:

1. Does the security team have full visibility across the application attack surface?
2. What AppSec tools are in place today? What gaps exist?
3. Are developers frustrated with the current AppSec processes because they cause coding delays or other headaches?
4. Are developers skipping security protocols because they are under pressure to deliver on time to market?
5. Is the executive or management team pressuring developers to bypass security processes in order to meet goals or deadlines?
6. Is the organization having problems scaling DevOps because of security gates?
7. Are specialized security experts required to deal with AppSec? Has your organization struggled to find, recruit, and retain these security experts? Are there security gaps as a result of the inability to do so?
8. Are developers and security team members overwhelmed in terms of alert fatigue caused by false positives?
9. What is the risk tolerance of the organization related to application vulnerabilities?
10. Are there vulnerabilities that matter more than others?
11. Are certain applications at higher risk than others?
12. Do your AppSec processes follow your applications from development into production runtime?

02

ESTABLISHING RELATIONSHIPS

"IF YOU SPEND TIME ONLY IN SECURITY LAND, YOU REALLY DON'T UNDERSTAND THE COMPLEXITIES THE BUILDERS GO THROUGH TO DELIVER."[11]

Once viewed as a back-office function, cybersecurity is now discussed in 89% of board meetings.[12] Everyone is a stakeholder in the cybersecurity program, and the CISO/CSO is now a peer to the CIO at many organizations.[13] This means that new CISOs/CSOs need to develop relationships across the organization from day one. This is especially true of the executive team and managers of key stakeholder groups. "Building a strong and effective professional relationship takes time and effort," says Walls of Visionworks. "It shouldn't be one sided, but rather a balanced relationship, established on trust and mutual benefit."[14]

WHICH DEPARTMENTS ARE MOST IMPORTANT?

New CISOs will do well to get off on the right foot with the following groups:

[11] Rohan Amin, CIO, Consumer & Community Banking, JPMorgan Chase, quoted in "Protecting the Business: Views from the CIO's and CISO's Offices," McKinsey, March 2020.

[12] "NACD Director's Handbook on Cyber-Risk Oversight,"National Association of Corporate Directors, January 11, 2017.

[13] "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.

[14] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.

- *Development and DevOps Security.* When it comes to AppSec, the executive in charge of the development team is a key stakeholder and controls one of the more important parts of the IT function at many organizations. Depending on the company's structure, the DevOps security function may report to either the CISO/CSO or to the development team. Either way, the CISO/CSO will need to ensure that the security and development functions work smoothly together without impeding one another.

- *Product.* Those creating the next generation of the company's offerings are necessary allies of the cybersecurity program, and they can help the CISO/CSO factor future security needs into current planning.

- *Sales and Marketing.* A solid relationship with those who bring a company's product to market helps the CISO/CSO understand what is driving customers—and by extension, the development teams tasked with providing them with a relevant experience. The application spend of sales and marketing leaders for cloud services and DevOps-driven applications is often more than that of the budget of the CIO in many organizations today. These applications are often competitive differentiators for businesses.

  Yet, as application development becomes more and more important for sales and marketing organizations, CISOs/CSOs must ensure they are aligned.[16] If not, these sales and marketing

"[A]S YOU HAVE THESE RELATIONSHIP BUILDING DISCUSSIONS IT'S IMPORTANT NOT TO PASS JUDGMENT ON ANYTHING YOU HEAR SINCE YOU MIGHT NOT KNOW THE POLITICAL UNDERPINNINGS OF THE INFORMATION THAT'S BEING SHARED."[15]

[15] Justin Fimlaid, "The First 101 Days as a New CISO—A Chief Information Security Officer's Playbook," NuHarbor Security, June 21, 2018.

applications, which typically store and transact personally identifiable information (PII) and other highly confidential data, can place an organization at serious risk due to unpatched vulnerabilities.

- *Compliance and Audit.* For the CISO, there are many opportunities to leverage compliance requirements to build substantial and mutually beneficial processes and procedures that make the organization more secure by filling in security gaps that increase risk. There also may be opportunities to reduce duplicative efforts to the benefit of both teams. Adopting a control like the National Institute of Standards and Technology (NIST) can bolster the CISO/CSO's credibility with this team while improving security.

- *Security Operations.* Without this team, applications may not be available for customers for long periods. CISOs/CSOs need to become familiar with this team's processes and procedures, especially when it comes to how they deal with threat alerts. Subject-matter experts on AppSec may need to help them enhance their processes to bring software security on par with traditional incident response.

- *Legal.* This team is an important ally and stakeholder, according to Brian Glas, assistant professor of Computer Science at Union University. "They need you and you need them," Glas asserts. "It's critical for a CISO to understand the legal perspective and potential benefits and ramifications for decisions made in the security realm. This team also keeps tabs of new regulations that may be coming, eliminating surprises for the CISO/CSO."

A couple of large, AppSec-related projects could help build the natural partnership—ensuring that the proper security terms and controls are included in contracts and securing the open-source/third-party dependency pipeline. The legal risks of including the wrong licenses are many times on par with the security risk of vulnerable dependencies.

[16] Laura McLellan, "By 2017 the CMO Will Spend More on IT Than the CIO," Gartner, accessed May 5, 2020.

03

APPSEC ON THE PRIORITY LIST

For a new CISO/CSO, AppSec security may not be the number one priority, but it should rank high on that list at many organizations. As the economy becomes more reliant on digital interaction with customers, partners, and employees, applications are the key to success. One recent study determined that access to developer talent is an even bigger factor in a company's success than access to capital.[17] Another study found that 68% of organizations have a mandate from the CEO that nothing should be allowed to slow down the development process.[18]

Such mandates address a very real problem in application development. Research shows that as many as 17 hours per week of developers' time is wasted because of inefficiencies—many of them security-related.[19] To compensate for this, 52% of respondents in one study admitted to scaling back security measures to meet a business deadline.[20] Helping development teams do their job without security-related delays sets the CISO/CSO up for success across the organization.

It is critical that the CISO/CSO work with the development team to align their shared vision and goals with overall company goals—and the organization's risk tolerance. "Remember, when treating risk, you have several options: remediate, mitigate, eliminate, transfer, or accept a risk," says Visionworks' Walls. "If mitigation

17 "The Developer Coefficient," Stripe, September 2018.
18 "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.
19 "The Developer Coefficient," Stripe, September 2018.
20 "52% of Companies Sacrifice Cybersecurity for Speed," Threat Stack, March 13, 2018.

is chosen for an AppSec risk, the fix can be technical and/or procedural in nature."[21] Technical fixes would include rewriting code to remove vulnerabilities, while procedural remediation would adjust DevOps processes to ensure that security is built into an application.

"APPLICATIONS ARE THE HEART OF MOST BUSINESSES AND THE TARGET OF MOST HACKERS; THEREFORE, SECURING YOUR APPLICATIONS IS CRITICALLY IMPORTANT TO YOUR EFFECTIVENESS AS A CISO, AND TO THE SUCCESS OF YOUR BUSINESSES."[22]

ASSESSING THE APPSEC LANDSCAPE

It is important that the new CISO/CSO understand where current processes and procedures fall short from an AppSec perspective as quickly as possible. A gap analysis can identify problem areas and inform the CISO's roadmap to address them. At the same time, CISOs/CSOs will do well to conduct a SAMM assessment to determine the organization's overall AppSec maturity level and set the next several phases of goals and measure via a dashboard.[23] This assessment can be done using in-house expertise or by a neutral third party.

According to Visionworks' Walls, it is helpful to visualize an organization's AppSec posture by looking at each component part:[24]

- *Governance.* Establishing policies, procedures, standards, measurements, and separation of duties for the program
- *Development.* Ensuring that the development process moves forward smoothly and securely, and that only authorized people are allowed into development systems
- *Production.* Security scanning, monitoring, and enforcement—and remediation of vulnerabilities

[21] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.
[22] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.
[23] "Software Assurance Maturity Model," OWASPSAMM," accessed May 5, 2020.
[24] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.

"51% OF COMPANIES HAD AT LEAST ONE BREACH IN THE PAST YEAR . . . [T]HE TOP THREE ATTACK VECTORS WERE A DIRECT ATTACK ON YOUR APPLICATION, TAKING ADVANTAGE OF A SOFTWARE VULNERABILITY, OR COMPROMISED USER CREDENTIALS."[25]

- *Management.* Performance monitoring and incident response
- *Infrastructure.* The infrastructure for on-premises and cloud security, high availability, and disaster recovery
- *Data Protection.* Encryption, access management, and key and certificate management

The priority is undoubtedly to deliver secure applications on an aggressive timeline—two goals that can conflict with each other if the company is still using traditional approaches to AppSec. However,more integrated and automated approaches make it possible to meet both goals.

[25] Stephanie Balaouras, "Cybersecurity in 2020: The Rise of the CISO," MIT Technology Review Insights, February 24, 2020.

04

QUICK WINS FOR APPSEC

While the new CISO/CSO does well to think strategically and focus on long-term outcomes, a few "quick wins" when it comes to AppSec can actually set the stage for success in these longer-term plans. Here are some challenging—but manageable—short-term goals that could help set the stage for a successful AppSec program:

- *Application inventory (Day 30).* As mentioned above, if such an information source does not yet exist, the CISO should assign team members to assemble one. While this needs to be started within the first 30 days, its completely will likely take longer.
- *Policy gap analysis (Day 60).* Ensure that detailed AppSec policies exist and that there is a process to review and maintain them. Involve stakeholders in formulating policies that are missing, and ensure that the new policies comply with standards such as NIST. Make a list of guidelines that are needed to align the technology and frameworks in use with these standards.
- *SAMM assessment (Day 60).* Conduct a formal assessment of the maturity of AppSec at the organization as an aid in planning next steps.
- *Risk mapping (Day 100).* Some applications are simply more business critical than others, and CISOs/CSOs should be deliberate about determining relative risk for various applications. A specific, written ranking of the risk posed by each application is doable in the first 100 days and can help provide a priority list for AppSec focus.

- *Developing an AppSec roadmap (Day 100).* This plan should envision a comprehensive, holistic approach to AppSec that builds on previous successes to advance the program's maturity. This plan should include incremental steps that provide repeated "quick wins" along the way, but with a strategic focus and direction in mind.

THE COST OF FIXING A SOFTWARE VULNERABILITY AFTER THE DESIGN PHASE:

- **6X MORE, IF FOUND DURING IMPLEMENTATION**
- **15X MORE, IF DETECTED IN TESTING**
- **100X MORE, IF IDENTIFIED IN PRODUCTION**[26]

[26] Mukesh Soni, "Defect Prevention: Reducing Costs and Enhancing Quality," iSixSigma, accessed April 9, 2020.

05

INTERNAL COMMUNICATIONS ABOUT APPSEC

Explaining security concepts in terms that regular people can understand is critical—whether the communication is to the executive team, the board, or to rank-and-file employees at a company. Cybersecurity professionals often use vernacular that differs from the language used in the rest of the business. AppSec is especially complex, and even developers who have a deep understanding of the technology that powers applications are not security experts—and do not want to be.

For communications outside the security team, discussions of risk should be framed in the way that the business defines risk. Below are some suggestions for how to communicate to different stakeholders during a CISO/CSO's first 100 days:

COMMUNICATING WITH THE BOARD

CISOs/CSOs have only recently begun having frequent opportunities to communicate directly with the board, and they should take advantage of their receptivity. If the CISO/CSO can present the company's security challenges in terms they can understand, the board can provide critical support for cybersecurity priorities. Visionworks' Walls asserts:

"BOARD MEMBERS DO NOT LIKE FUD—FEAR, UNCERTAINTY, AND DOUBT."[27]

"Board members do not like FUD—fear, uncertainty, and doubt. Therefore, present your current application security posture in a solution-focused way, emphasizing the actions you are taking to improve your security posture and reduce risk, rather than saying, 'the sky is falling.'"[28]

COMMUNICATING WITH THE EXECUTIVE TEAM

CISOs tend to work with their fellow executives on a regular basis, and it is easy to forget that they do not have the same familiarity with cybersecurity lingo that security team members have. As with the board, CISOs should frame communication with the executive team in terms of how AppSec drives the business. Many executives may understand the benefits of DevOps without a full comprehension of the security risks—but they probably hear about it when security processes slow down development. When CISOs/CSOs move their organizations beyond legacy approaches to AppSec to a more integrated approach, they can promote the results: reduction in downtime, greater efficiency for the development team, and avoidance of breaches and other security incidents.

COMMUNICATING WITH RANK-AND-FILE EMPLOYEES

As Ravinder Arora, CISO at IRIS Software, contends, "An organization's security culture requires care and feeding."[29] Accordingly, CISOs/CSOs also need to communicate their priorities across the company to a diverse set of workers. As a start, they should ensure that AppSec is a part of the cybersecurity awareness training curriculum. Beyond that, as the CISO is becoming familiar with the company, it might make sense to conduct a roadshow to promote software security and actively solicit feedback and requests from teams and

[27] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.
[28] Private correspondence with Sean Walls, VP and CISO, Visionworks of America, Inc.
[29] "'An Organization's Security Culture Requires Care and Feeding'," CISO MAG, March 3, 2020.

departments. This communication should not rely on geek-speak or techno-talk, but should describe the problems—and potential solutions—in plain language.

COMMUNICATING WITH DEVELOPERS

When communicating with the organization about new AppSec initiatives, special focus should be placed on the development team. New CISOs/CSOs frame their proposals for new approaches to AppSec in terms of how it makes developers' jobs easier. If the perception among developers is that security impedes them from doing their job, they will be very receptive to a solution that eliminates security-related delays and reduces the frequency with which they must deal with the security team. Providing superior security while simplifying the development process will be an attractive proposition for this team.

"AN ORGANIZATION'S SECURITY CULTURE REQUIRES CARE AND FEEDING."[30]

[30] "'An Organization's Security Culture Requires Care and Feeding'," CISO MAG, March 3, 2020.

06 CONCLUSION

The new CISO/CSO clearly needs to run a marathon rather than a sprint, but success in the first 100 days sets the cybersecurity team up for success in the long run. It would be nice to build out a fully functional AppSec program in the CISO/CSO's first quarter, but everything cannot be done immediately. Like a long-distance runner, the CISO/CSO must move at a deliberate pace, assembling a strategy and vision in the first 100 days that will guide the team's activities for the next year or two.

This strategy should align with the company's goals, adhere to the way it manages risk, and be consistent with its brand identity. The CISO/CSO should secure support for the new plan from fellow executives, the board, and a critical mass of the rank and file. Remember, security not only protects a company's assets, but if done right, it can enhance an organization's brand, be a differentiator, and empower the business.

"APPS HAVE BECOME *THE* BUSINESS IMPERATIVE, *THE* KEY CONDUIT TO CUSTOMERS AND *THE* ESSENTIAL BUSINESS ENABLER."[31]

[31] Jo Peterson, "DevOps: The Secret to Doing More, Faster, Better and for Less Green," Channel Futures, February 23, 2018.

SPECIAL THANKS

This Management Guide was compiled with the support and feedback of Sean Walls and Brian Glas. Their insights and recommendations were critical in the compilation of the guide, though neither is responsible for any errors or omissions contained therein.

Sean is the VP and CISO at Visionworks of America, a leading provider of eye care services in the United States with 700-plus retail locations in more than 40 states, over 600 optometry clinics, and two lens manufacturing plants. Sean has more than 20 years of experience in cybersecurity, has spoken at numerous conferences, appeared in various podcast shows, and touts a long list of credentials (CISM, CCISO, CCSK, CEH, CISA, CCSP, CCNP, GCIH, GWAPT, QSA, and MCSE).

Brian is an assistant professor of Computer Science at Union University and possesses nearly 20 years of experience in application development and cybersecurity and is a frequent subject-matter presenter at industry events and conferences. Additionally, Brian was one of the project leads for and is an active contributor to SAMM and the OWASP Top 10.

CONTRAST SECURITY
240 3rd Street
Los Altos, CA 94022
888.371.1333

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.