Smartest path to DevSecOps transformation

Coalfire Cloud Advisory Board contributions by
Jerry Bell, IBM Public Cloud
Gail Coury, F5
Adrian Mayers, Premera Blue Cross
Nils Puhlmann, MoonPay and Cloud Security Alliance
Matt Sharp, Logicworks
Tony Spinelli, Urban One, Inc.
Mark Weatherford, AlertEnterprise and National Cybersecurity Center
Contents

Meet the experts ................................................. 2
The challenge ......................................................... 5
01 Preparation ....................................................... 7
02 The secure development lifecycle ...................... 11
03 Culture ............................................................. 15
04 Automation ......................................................... 19
05 Governing the organization ................................ 25
06 Reporting .......................................................... 30
07 Security as a differentiator ................................ 34
Conclusion .......................................................... 38
Coalfire co-authors ................................................. 39
Meet the experts

**John Dickson**

*Vice President, Security Solution Architecture, Coalfire*

John is an internationally recognized security leader, with 20 years’ experience in intrusion detection, network security, and application security in the commercial, public, and military sectors. A former U.S. Air Force officer, he served in the Air Force Information Warfare Center and was a member of the Air Force Computer Emergency Response Team. He has played pivotal roles with companies including Denim Group, Trident Data Systems, KPMG, and SecureLogix Corporation.

**Jerry Bell**

*CISO and Vice President, IBM Public Cloud*

Jerry has been slinging code, managing systems, modeling threats, and hunting down vulnerabilities for 30 years. Jerry has seen it all. Although he’s always learning, nothing in his career has come close to the disruption of the cloud, and with it, the need to learn more, faster. The cloud’s impact on the development and the expansion of risk exposure and fundamentally new capabilities for risk mitigation compels CISOs and InfoSec professionals to adapt to faster learning curves and implement novel approaches to development lifecycles.

**Mark Weatherford**

*CSO, AlertEnterprise; CSO, National Cybersecurity Center; board advisor to public and private organizations*

After a 26-year career as a cryptologist in the U.S. Navy, Mark retired and joined a defense contractor to build and operate the Navy’s first enterprise SOC. Among other positions on a resume too long to list here, he became the first CISO for the State of Colorado and worked with Coalfire Founder Rick Dakin to write the state’s first InfoSec policy. It was the first legislation of its kind to be passed by a state government and established Colorado as a leader in cybersecurity. Following Colorado, Weatherford was lured to California where he once again became the state’s first CISO, this time working with more than 160 state agencies and departments. Then the White House called, and he was appointed as DHS’s first Deputy Under Secretary for Cybersecurity.

**Adrian Mayers, Dr.B.A.**

*CISO and Vice President, Premera Blue Cross*

As the current CISO of Premera Blue Cross, with seats on 10 security advisory boards, and as an alumnus of Nokia and Vertafore, Adrian’s professional experience signaled to him the coming long-term upheaval caused by digital transformation. He has managed enterprise security programs for the past 20 years and his extensive understanding of cyber policy gives him the unique perspective of the landscape both up close and geopolitically.
Meet the experts

Matt Sharp
CISO, Logicworks

Matt recognized the upside in digital transformation early. First, he got his MBA, then he refactored his career around DevSecOps in the public cloud. Matt’s success as a security professional comes at the heels of a dogged persistence and intense discipline. Prior to his current role, Matt partnered to build a global InfoSec program and today he is helping others create and protect digital business value.

Nils Puhlmann
CRSO, MoonPay; Co-founder, Cloud Security Alliance

Nils has been questioning the status quo for his entire career. His resume in brief includes security executive leadership roles at five public companies, pivotal positions in two IPOs, and numerous industry board positions. His passion is conveyed through the dedication of his spare time to giving back to the community and challenging the accepted thinking in security. For example, he co-founded the Cloud Security Alliance in 2008 to ensure that the speed of technology innovation did not blindside the security industry again. He’s built security programs and teams at scale and has focused on coaching and building future security leaders. The hallmark of his professional style is thinking bigger. He’s been looking to the future of technology and security since most of us were on dial-up and he’s not going to stop any time soon. To this day, he enjoys applying and adjusting security principles at companies that disrupt existing industries.

Tony Spinelli
CSO, Urban One, Inc.; Board Director, Peapack Bank, Blue Cross Blue Shield

From pioneering global security practices at Ernst & Young a quarter century ago to leveraging AI/ML into cloud security strategies at Urban One today, Tony has had a hand in shifting every paradigm since the dawn of cyber history. He was there when First Data set the table for secure electronic payments; when Tyco pioneered the movement to public cloud operations; when Capital One was the first bank to go cloud-native; and pretty much everywhere in between, before, or since.

Gail Coury
CISO and Senior Vice President, F5

Math was Gail’s favorite subject. She pivoted from wanting to be a math teacher to getting a Computer Science degree, and the result has been a long and influential career in application development and security. From one of the software industry’s most significant M&A ventures starting in the ‘90s with JD Edwards, Peoplesoft, and Oracle, to today as CISO at F5, the world is cyber-safer thanks to Gail’s contributions. She continues to shape future generations of cybersecurity through her devoted advocacy of Women in Tech.
The challenge

By John Dickson, Vice President, Security Solution Architecture, Coalfire

The secure CI/CD journey

The Coalfire Cloud Advisory Board (CAB) represents the first generation of cybersecurity pioneers that has paved the way from data center perimeter defense to where we stand today, poised on the brink of risk-based security strategies and cyber market expansion in the cloud.

As leaders and innovators, the CAB helped make history by setting the standards and establishing security and compliance best practices at every turning point. Our advisory board has seen it all, and together they see today’s top priority - application security - through hard-earned wisdom informed by experience.

Software development lifecycle (SDLC) history

Shortly after Coalfire was founded 20 years ago, Microsoft found itself losing customers. Bill Gates confessed in a famous internal memo that too many viruses, malware, and the near fatal error of treating security as an afterthought were eroding market trust for his company. He saw the need to build security directly into the company’s products, and the concept of secure software development lifecycle was born.

The Coalfire CAB sees that journey continuing today, and that the time has come for the final “shift left” in embedding security into the alpha stage of development. We’re not quite there yet, and this report is designed to help DevSecOps establish the new app dev methodology where security is baked into every digital product roadmap from the very start.

In a world where product lifecycles are defined and impacted by continuous integration and continuous delivery, and where applications, containers, and even bare metal servers and legacy workloads are connected and scaling dynamically in public clouds, this final phase of the paradigm shift has to happen within every enterprise.

Agile evolution

It’s understandable it would take some time for designers, developers, and engineers to implement a security-first mentality in the early waterfall and later agile processes of application creation. Even if not an afterthought anymore, security controls are typically not the first thing an inventor thinks of when tackling a CXO-driven imperative to fill a customer need. Not to mention that designing, developing, and deploying digital products was never going to be easy in a reconfigured global economy after pandemic shutdowns.
The good news is that DevSecOps leaders are getting the job done. The problem is, with the proliferation of digital solutions and the explosion of cloud commerce across expanding attack surfaces, public awareness of cyber risk has gone through the roof. Risk tolerance between buyers, sellers, and suppliers is cratering to virtually zero. Customer trust is wearing down with the daily headlines. Buyers and suppliers sense rising, direct risk exposure, and are more likely to vote with their feet by running away from compromised companies.

Executive solution

With heightened urgency, boards and C-suites must move their organizations faster on the adoption curve by mandating new product security imperatives, and by allocating the human and financial resource requirements to get this done. In addition, directors and officers need to step up and make the business case to shareholders, and market their companies’ trust value to customers.

The CAB mutually agrees that executive leadership teams need the help of CISOs, CIOs, and developers to enlighten management toward application security, now its most mission-critical IT directive in the age of digital transformation.

With this report, the Coalfire CAB and cloud security thought leaders from Coalfire bring our best ideas and up-to-the-minute perspectives on everything from secure product lifecycle best practices to creating risk-based cultures that use security as a go-to-market enhancement tool. After all, security is no longer a trade secret – it’s an out-front brand positioning statement.

Executive leadership teams can’t do this alone. Nor can security teams. Developers must adjust and embrace responsibility in the final shift left. IT must defend as we code, and meet engineers in the right places at the right times with tools and budgets to leverage security into all phases of product development.

Securing the enterprise now starts and ends with the digital services provided. Securing those solutions, from idea to auto-scaling in the cloud, is the new prime directive.

We hope this report, with the combined wisdom of the Coalfire team and our esteemed CAB, will help today’s generation of cybersecurity pros step up, take charge, and help take their company’s products to the promise of a secure cloud.

Top challenges in secure cloud application development

1. Skills shortage
2. Third-party dependencies
3. Configuration automation
4. Vulnerability management
5. Remediation management
6. Support for multi-cloud
7. Shadow IT
8. Vendor/supply chain dependencies
DevSecOps is not optional

Developing secure applications requires an organization to embrace the value and importance of security and requires alignment from the board down to the developer. Leadership support is critical to building a solid DevSecOps foundation and programs are most successful when training and automation support the organizational vision.

10-second takeaways

As you prepare for your DevSecOps transformation, ensuring proper focus and investment in these areas is key:

- Define and align your security vision.
- Commit to train, train, train.
- Plan for, and invest in, automation.
- Enlist an AppSec champion for support and scalability.

“It’s the CISO’s job to create momentum on these initiatives, arrive at agreement, and integrate a means of measurement with every policy and procedure.”

Mark Weatherford
CSO, AlertEnterprise
CSO, National Cybersecurity Center
Board advisor to public and private organizations

Co-authored by Patrick Kehoe
Chief Marketing and Strategy Officer, Coalfire
The imperative to mature DevSecOps

Automating around application and vulnerability management systems across a wide range of integrated tools is the new security imperative and is leading to a convergence in the secure product space. Organizations must create a new vision for everyone to follow across all components of the technology infrastructure and then commit the resources needed to ensure that the concept of maturity is clearly defined for their organization.

How CISOs communicate their vision

1. Gauge security awareness and interest with the organization’s leadership.
2. Articulate what “secure” means, why you want to be secure, and get others to believe.
3. Coach fellow managers and executives into alignment between security and C-suite teams.
4. Cultivate a regular audience with the board, and get them on board.
5. Establish expectations, policies, and a culture that orbits around security.
Training

Training programs are often seen as distractions, and developers hate being interrupted. However, training improves productivity and upskills developers. Security training is a critical – and ongoing – priority for your application development team.

Get training right

- **Make it quick and convenient** with sessions that are short and easy to attend.
- **Develop skills and make it fun.**
- **Encourage subtle competition** between product development teams.
- **Integrate training between development and security** to bring them closer to becoming a unified team.
- **Ensure training is mandatory** for everyone including managers, designers, engineers, etc.
- **Bring in third-party trainers** to reinforce new skills and methods.
- **Encourage developers to build skills**, add qualifications to their LinkedIn profiles, and become stand-out experts in their job.

Automation

Application security orchestration and correlation (ASOC) helps DevSecOps teams improve their functionality by streamlining tools that correlate, discover, and de-duplicate disparate testing results; validate and prioritize vulnerabilities; and manage remediation. This layer of correlation between application development, compliance, and testing is key to integrating security and taking a shift-left step in achieving true secure product development.

Not too many years ago, management and developers thought that security was simply an annual check-in-the-box requirement and a primary roadblock to productivity. Unfortunately, some people still think about it through that misguided lens. The cloud, the mainstreaming of CI/CD, and continuous security assurance has resulted in market demand that requires organizations to fully operationalize DevSecOps.
Enter the AppSec champion

In the last decade, security leaders have observed the emergence of application security champions programs (known also as “AppSec champions programs”). Security leaders use them to influence software developers in their organization to write software in a consistently secure and scalable way. Within organizations, these champions are referred to as ninjas, embeds, or security satellites, but they share common attributes:

• They are led by a smaller AppSec team operating out of a centralized security organization with little formal organizational control over the software development efforts.
• They exercise influence more than managerial control to affect the behaviors of software developers who report to managers in a separate reporting line.
• They are organized informally and exist despite there being no formal mandates or structure, originating within security organizations – not from the top of the organization.

AppSec champions programs are not training programs for developers. This is particularly important, as the number of software developers within an organization dwarfs the number of security staff focused on application security. They employ concepts like managerial leverage to enable developers to do what the security teams themselves cannot do – consistently build software that is more resilient, more defensible, and less vulnerable. They have the potential to change the behavior of their development peers, thereby improving the security of software produced within their organization.

Security is no longer downstream of creative product invention and application development, but rather integral to the process. It’s time to model the threats, identify and fix vulnerabilities faster, embed security into every aspect and at the earliest stages of the application development cycle, and never look back.
Risk-based development without end

I came to IBM through its acquisition of Internet Security Systems in 2006. That was back in the good-old, pre-cloud days when development teams worked in labs buried deep within internal networks. We felt more sheltered from the outside world, and no one bothered us much. The security blast radius that could hurt the organization was at least somewhat contained behind our firewalls, and little of what we did drew the attention of managers and customers, let alone the media. Of course messes were made back then, they were just less noticeable and easier to clean up than they are today.

10-second takeaways

- Inject security from the outset.
- Embrace the mindset that attacks are inevitable.
- Build executive buy-in by tracking business KPIs (not just security KPIs).
- Mitigate risks before writing code by threat modeling.

“Whatever tolerance we had for failure has been turned upside down in the cloud.”

By Jerry Bell
CISO and Vice President, IBM Public Cloud
Co-authored by Caitlin Johanson
Director, Application Security Services, Coalfire
Modern dev discipline

The increased risk exposure and expanding attack surfaces in hyperscale, multi-cloud environments have virtually eliminated the margins of error we used to take for granted, as a number of organizations have very publicly and painfully discovered.

There's no turning back on the cloud. Why? Because its fundamental purpose of existence is to reduce the friction of IT consumption and commerce. Many product development teams are simply not used to the continuous creation and destruction that cloud workloads deliver, but they need to be. At the same time, operating in the cloud provides security and resiliency capabilities that we could only dream of in those good old days. Our challenge as CISOs is managing those emerging risks while taking full advantage of transformational security capabilities offered by the cloud.

Though somewhat antithetical to the agile method, security must be injected into the first sprint, and within every scrum and epic thereafter. The cloud is the force multiplier, driving the final leftward shift to a best-practice methodology of DevSecOps, as well as the continuous integration and deployment of security into development lifecycles.

The most impactful approaches for embedding security into the SDLC

- Executive buy-in/support
- Dedicated application security resources
- Shift-left security (DevSecOps)
- Defined secure coding standards
- Secure SDLC maturity roadmap
- Application security testing gates
- Cross-functional communication/collaboration
Risk-based chaos

Attacks are inevitable, and we must manage our security operations and development processes accordingly. The cybersecurity dog is never going to quite catch the cyberattack cat, and there are no safe spaces or tranquility in our futures. Organizations must operate under the constant, urgent momentum of prevention, detection, and response.

Though a defense contractor is going to face different threats than a consumer-facing retailer, just about every modern business has a few things in common, other than the priority to stay in business during and after a disruption.

The reality is that the perception of risk is more differentiated than the actual risk itself. CISOs need to develop intuition around the threats facing your organization and be able to clearly articulate to executive leadership why your view of risk needs to be prioritized, and why it must be integrated at the forefront of product lifecycles.

There’s no “easy button” with secure development lifecycle. Like the 88 keys on a piano, there are millions of sounds and inflections that can be produced, and though incalculable, there’s still a limited framework that the musician must work within.

Common threats to business:
- Continuity after disruption
- Privacy protection
- Stock price/market value
- Ransomware
- Logistics
- Supply chain
- Sketchy/superficial vendors
- Stolen trade secrets
- Nation-state actors
- Brand reputation
Executive buy-in and belief

CISOs need to be able to show others - often non-technical people - that they understand the priorities that are idiosyncratic to the business, and that they can make the case for provisioning and budgeting security's role inside of and integral to the product development process. Be good at math, but also good at psychology.

By conducting a stakeholder review, business objectives will rise to the top, which in turn will help set precedent and priority for identifying development lifecycle vulnerabilities and managing against their perceived threats.

Threat modeling and DevSecOps architecture

While threat modeling is the key to integrating security into the development lifecycle, it’s also where we’ve seen the most corners get cut. Threat modeling is thinking through how everything from an entire system to a single line of code can be attacked, then ideally mitigating those threats before writing the code. DevSecOps needs to instill the continuous demand for continuous risk prioritization, security scanning, testing, and remediation. Annual pen tests and periodic compliance checks should become far less relied upon if your environment achieves this level of automation.

This approach trickles down to help establish protocols within software development teams, making security checkpoints part of foundational code development. Repeating the secure product mantra brings home the point and sets the right tone for what happens in the cloud: Everything scales. Continuous, dynamic development across the business is the new norm.

Threats can be modeled, but every single threat cannot be accounted for. Intuition, logical thinking, feeling, choosing, and playing the right notes work together to secure not only the software development lifecycle, but also the lifecycle of the organization itself.

Best metrics for AppSec program success:

- Number of high/critical vulnerabilities found in the development process
- Number of high/critical vulnerabilities found in production
- Recurring vulnerabilities found in the development process
- Number of incidents/service disruptions caused by security issues
Creating a risk-based mindset within your organization

Arriving at a risk-based product development lifecycle requires creating a risk-based culture. You can automate just about everything these days, but the source code for early-warning risk management starts with people and teams, not machines.

10-second takeaways

- Identify which internal obstacles may be causing issues and how to manage pervasive cultural habits.
- Rely on the cultural triad (partnership, cooperation, and collaboration) and plan to build from the ground up.
- Focus your efforts to build culture on shared goals and outcomes between security and IT teams.
- Articulate security-first messages as customer-first messages.

“Security has to be the one to come in and assume they are not wanted.”

By Adrian Mayers, Dr.B.A.
CISO and Vice President, Premera Blue Cross

Co-authored by Mike Eisenberg
Vice President, Strategy, Privacy, and Risk, Coalfire
Naming and taming the obstacles

Creating a culture within any organization requires understanding the obstacles and turning them into opportunities. The priority is to identify and label the challenges. This common language will enable teams to quickly identify and determine relics of previous cultural norms.

Many sources of friction share common origins:

- Software development has worked in its own silo for generations (traditional DevOps may prefer this paradigm, with little or no security involved).
- Sophisticated compliance frameworks and rising privacy issues have gained more attention.
- The growing threat landscape endangers customer data through the applications and digital products themselves, not just at the network level.

While DevSecOps can address risks within the SDLC, it doesn’t often cleanly align with legacy development approaches. CISOs play the pivotal role to bridge the needs of the organization and the team members who must embrace an entirely new way to operate every day. Point-in-time security has given way to continuous integration/continuous deployment (CI/CD), which requires alignment across more functional teams than ever. A thoughtful approach to creating a culture that can thrive in this new operating model is crucial to any organization’s success.

“Personal pride in someone’s work can’t easily be measured, yet a single individual’s attitude is the single most important cog in the system that makes the culture work.”
The cultural triad: partnership, cooperation, and collaboration

**Partnership**
- **WHO**
  - Engage with peer-to-peer respect and enter with empathy and a listening/learning mindset.
  - Be fair to everyone, but let’s start with being fair to the customer.
  - Start the conversation with designers, developers, and engineers from the customer’s threat perspective.
  - Provide buyers with assurance. If they don’t get it, they’ll find somewhere else that provides and certifies it.

**Cooperation**
- **HOW**
  - Clarify and delegate ownership and accountability.
  - Understand that development may have legitimate grievances with security or executive leadership.
  - Use organizational purpose and mission to reframe the context of “why” and “how” to develop respect and build trust.
  - Turn the conversation into how the DevSecOps process affects managers and their direct reports.
  - Understand that developer culture places tremendous value on quality.
  - Merge security with quality and infuse it into company culture.

**Collaboration**
- **WHY**
  - Strengthen the business value proposition and enhance job security with cross-functional collaboration.
  - Build and embrace the new culture to empower employees with more portable skills, enabling career evolution and promotion.
  - Secure applications to drive revenue and enable business functions like mergers and acquisitions.
  - Adopt the risk-based culture within DevSecOps to promote healthy competition, purpose, and pride within teams and instill confidence in their ability to code securely.
  - Enable, improve, and build cultural diversity, equity, and inclusion. Culture should be a mosaic of the company and the customers it serves.
Customer-first is security-first

It’s our responsibility as security leaders to craft messages that focus on security, while placing our customers’ needs first. Building programs that create a win-win scenario through a security-first initiative will help drive a customer-first objective. Below are a few examples of how this might work.

<table>
<thead>
<tr>
<th>Security-first</th>
<th>Customer-first</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure coding practices</td>
<td>Meets customer-required security standards</td>
</tr>
<tr>
<td>Static or dynamic code analysis</td>
<td>Reduces application security vulnerabilities</td>
</tr>
<tr>
<td>Application penetration test</td>
<td>Identifies and remediates known vulnerabilities</td>
</tr>
<tr>
<td>Risk-based code analysis</td>
<td>Enables business-aligned risk treatment</td>
</tr>
<tr>
<td>Assigned security advocates or AppSec champions</td>
<td>Creates cultural cybersecurity points of contact</td>
</tr>
</tbody>
</table>

Ultimately, we all want to achieve the same objectives

Secure products have become value propositions and trigger points for purchasing decisions. The secure product lifecycle is closer to everyone’s core business than ever, and everyone knows it. Customers expect it, and marketing is talking about it. Security has become more cross-functional by necessity, and with it, the surrounding corporate culture that supports it. A risk-based culture focused on threat modeling and the logical prioritization of vulnerabilities makes all this possible.
Leveraging DevSecOps to get products to market faster

Developers and security teams are automating cybersecurity. Annual compliance checks, audit teams, and physical offensive testing may never go away, but in the cloud, regulatory frameworks, attack surfaces, and product development are converging in perpetual motion. The cloud orchestration layer is a software-defined network and application environment that is our new playing field of automated solutions and managed services.

10-second takeaways

- Align and work closely with customers to understand how automation best supports their needs.
- Expand automation use cases.
- Prioritize automation from the top down to instill organizational willpower for secure SDLC.

“Managing risk in the move to the cloud is, frankly, more important right now than managing costs, and any organization that wants to move to the cloud to save money has the wrong idea.”
Customer-first mindset

Years ago, we anticipated customers would achieve high levels of automation in short order. We imagined that most customers would jump at the opportunity to deploy code multiple times per day. We reasoned that that would require us to repave and rebuild their environments on a constant basis. We started building tools that would allow our customers to integrate with us in this futuristic world, but we learned pretty quickly that most customers were simply nowhere near ready for the DevOps maturity we anticipated they would adopt.

Now, we certainly observe a rising customer desire for distributed, immutable, containerized, or serverless environments.

In reality, five years ago, very few customers had basic automation or requisite organizational structures to support fully automated code deployment. Now, we certainly observe a rising customer desire for distributed, immutable, containerized, or serverless environments. Still, not everyone is immediately sure how to get there. To facilitate customers’ pursuit of competitive advantages, our leaders continue to collaborate with customer dev and sec teams, taking one bite at a time. We’ve found ways to meet customers exactly where they are in their journey, and help them elevate their game at a pace that’s right for them.
The risk-based standard

In 2019, I struggled to find 150 people out of 50,000 at the RSA conference who were interested in DevSecOps. In 2022, I expect that number to be closer to half of all attendees. Managing risk in the move to the cloud is, frankly, more important right now than managing costs, and many organizations that want to move to the cloud primarily to save money have the wrong idea. The main reason that cloud migration isn’t necessarily an exercise in cost saving is because the opportunities of digital transformation are so vast. Expansive, disruptive thinking stemming from an abundance mentality means leaders are seeking to create and capture unprecedented value. So, every organization must adapt its risk management by modeling the threats and remediating the vulnerabilities that are most likely to affect value engines. No one size fits all. The answers will vary widely and cannot be neatly categorized or easily aligned with an off-the-shelf set of governance and operational standards. The cybersecurity opportunity in the migration journey is to lock in on a whole new set of more continuous, custom, and automatic security controls as the transition unfolds.

Automation is the way we reduce risk. It reduces human error.

No one size fits all

Every company’s cloud migration journey is unique and the solutions are likely to mirror the structure of the organization’s foundational communication structure.
DevSecOps methodology

When it comes right down to it, the aggregation of infrastructure-based vulnerabilities is converging around secure applications development and deployment. CISOs are implementing this automation transformation through cultural shifts between security, DevOps teams, and the C-suite. This is enabling a new way to do business that will have far-reaching impacts into the boardroom in years to come.

Security processes need to keep pace with the modern software development lifecycles that have emerged in the wake of broad adoption of agile software development. This means developing a holistic approach that leverages technologies and automation to complement software development activities. In practice, security processes must be implemented in a layered approach and sequenced within the CI/CD pipeline to find, reject, and/or fix vulnerabilities. Ideally, this happens automatically at a scale and speed that matches an organization’s vulnerability budget and risk appetite.

Organizations should create shared source code repositories to develop, constrain, track, and distribute pre-configured modules that are certified against standard compliance and security frameworks. Doing so allows organizations to take advantage of battle-tested reference architectures that unify their compliance initiatives and establish repeatable patterns that significantly streamline secure software development.

Vital to a resilient DevSecOps program is a capability to provide both development and operations teams with timely feedback as code is developed, so they can detect and remediate security issues as part of their daily development activities before context switching is required. To do this, security teams must heavily rely on automation.
Automation use cases

Consider the following development-stage security integrations in your cloud-native application lifecycle:

**Goals of continuous monitoring** (operate and monitor)
- Apply controls that segment inter-workload/container communications and access.
- Auto scale the environment based on customer demands and workload requirements.
- Implement effective patch and vulnerability management strategies.
- Identify and detect anomalous activities.
- Apply controls that support incident response activities.
- Collect governance artifacts and automate traceability.
- Continuously monitor system health and performance.

**Goals of CI/CD** (build and test)
- Create a bill of materials for each source code branch.
- Manage and inventory dependencies.
- Harden Amazon Machine Images (AMIs)/virtual machines (VMs) and containers to established security baselines.
- Collect governance artifacts and automate traceability.
- Identify and remediate misconfigurations and vulnerabilities within a lower run-time environment.
- Identify and remediate environment availability concerns.

**Goals of continuous deployment** (release and deploy)
- Reduce down times/interruptions for production systems (availability).
- Perform security configuration checks for cloud-native services.
- Validate that secrets are adequately secured.
- Perform checks against serverless functions to reduce attack vectors and security weaknesses.

**Goals of continuous development** (plan and develop)
- Embed security perspectives (from the start) into the product design and configuration management processes.
- Identify risks and threats.
- Develop and maintain repositories for good, known technical assets (application code, infrastructure-as-code [IaC], AMIs, reference architectures, etc.).
- Automatically identify misconfigurations and vulnerabilities within development workstreams.
- Receive (near) real-time alerting when security and functional inspections fail.
Automation case study: IaC security

The challenge
The adoption of a shift-left approach to the development and management of cloud infrastructure requires an approach similar to traditional application code development processes. Gates within the CI/CD process need to be established to detect security and compliance misconfigurations early in the development process.

The solution
Use IaC scanning tools that provide linting capabilities to inspect and analyze IaC as it’s developed. Pre-built policies examine the code for misconfigurations and provide engineers with the necessary steps to remediate issues before the code is moved to production.

The outcome
• Security and compliance considered from the start
• Consistent architectures and design patterns enforced
• High-severity events in product environments decreased
• Misconfigurations fixed early and fast
• Value creation balanced against risk

The time is now
Get started with alignment between the CISO and fellow CXOs. Organizations must teach and share knowledge from the top, look at what’s ahead, and examine the full spectrum of decision-point information. From the top down, move forward with that buy-in and full support from above. This instills the willpower to secure product development lifecycles that eventually get us to our automation destination.

The big takeaway? Automation is a competitive differentiator. Leave it alone, make it a low priority, or procrastinate, and you’ll be left behind.

Automation is a competitive differentiator. Leave it alone, make it a low priority, or procrastinate, and you’ll be left behind.
Governance must include centralized accountability and shared responsibility

Security is the biggest risk to business today. It’s the fastest way to take a company down. With the stakes so high, managing security programs has become one of the hardest jobs in the enterprise.

Many organizations presume that simply aiming for a risk-based approach to security will make governance obsolete. The reality is that there is not yet a tried-and-true governance model for security. There are best practices and concepts from more mature business disciplines like finance that could be applied, but the aim is to create shared responsibility for security outcomes and ensure that it includes both quantitative and qualitative measures.

To all directors, officers, shareholders, and security leaders: It’s time to stop presuming that it won’t happen to you and address security as the existential risk that it is. To do that, you must treat security not as a series of problems to solve but as an essential discipline that touches every part of the business. Security can easily threaten the resilience of the enterprise; therefore, it must become a part of everyone’s job responsibilities. For this reason, it’s imperative that ownership of this critical executive function has a seat at the CEO’s table and an ongoing partnership with the board.

10-second takeaways

- Insist on centralized accountability for security, starting at the board level.
- Incorporate qualitative metrics for comprehensive security dialogue. While countless organizations rely solely on quantitative measures, there is an enormous gap in looking at security this way.
- Embrace the idea that having security expertise in your organization is not the same thing as governance and commit leadership to the cause through a shared responsibility model.
- Require a cultural shift away from “moving fast and breaking things” to prioritizing quality and completeness.

“It’s time to stop presuming that it won’t happen to you and address security as the existential risk that it is.”

By Nils Puhlmann
CRSO, MoonPay
Co-founder, Cloud Security Alliance
Co-authored by Matt Klein
Field CISO, Coalfire
The enablers of good governance

Asking the right questions

In the boardroom, the normal response to issues surrounding finance and operations is usually analytical and data driven. The traditional CEO/CFO/COO's knowledge is built on business practice precedents set generations ago, and they enjoy an established, direct path to the board.

Similarly, when the topic of security comes up in the boardroom, the conversation is expected to be primarily data driven. This approach nullifies the value of looking at security the same way we look at customer experience and product development itself. Balancing qualitative and quantitative results to measure success isn’t new to organizations. Integrating metrics that can be viewed over time with discussions about indicators of security program health and maturity present a richer picture and enable in-depth dialogue about progress and improvement. Examples of this balanced method include:

• “Shift-left” effectiveness often has as much to do with cultural improvements as it does development discipline

• Security awareness training is most often done for compliance; however, it does not accurately reflect whether employees truly feel that they share the responsibility for the resiliency of the organization

• Increasingly, engagement scores like NPS have become a more important measure of quality of a service than its pure technical functionality

The board should be asking questions that uncover the full picture of the state of security in the company. These questions must go beyond the metrics and must filter down to every discipline.

Critical questions to ask in every executive security conversation:

- Do employees embrace the concept of security and are they incentivized to do so?
- Do you feel that the company is taking security seriously?
- Do you have the resources you need to create a mature security program?
- How would our customers feel if they knew everything we are doing or not doing to keep them secure?
Getting skin in the game at the board level and across the management team

Directors learned from the Enron debacle that board members can be held liable for allowing malpractice to result in damaging outcomes. There was a pervasive culture of cheating and fraud that enabled the behavior to continue. Leaders can be banned from future board positions, held personally accountable for legal damages, and face other consequences. If you’re on an audit committee and you discover misconduct or illegal activity, you have a duty to act. Sarbanes-Oxley was the harsh governance that came out of this tragedy, and we haven’t seen another Enron-scale event since.

Having learned from the past, the board should appoint the member who has the most operational experience with security (think: audit committee expertise) and they should engage the CISO for support in defining responsibility for the topics that comprise security. These two must work together to ensure that security becomes part of the DNA of the organization itself. This working pair should establish the questions – and criteria – across each area of the company that outline what a strong and mature security program looks like.

Understanding risk and security in qualitative terms

<table>
<thead>
<tr>
<th>Leadership role</th>
<th>Qualitative questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO and board</td>
<td>Can you articulate how the company is taking security seriously, and why?</td>
</tr>
<tr>
<td>CFO</td>
<td>Is the investment in the security program sufficient to ensure the resiliency of the enterprise, and why?</td>
</tr>
<tr>
<td>COO</td>
<td>How long could the organization sustain an outage due to a cyber incident?</td>
</tr>
<tr>
<td>CTO</td>
<td>How long does it take the incident response process to address known data breaches?</td>
</tr>
<tr>
<td>CPeopleO</td>
<td>How do employees embrace the concept of security, and are they incentivized to do so?</td>
</tr>
<tr>
<td>CMO</td>
<td>When a cyber incident and its sensitive details are made public, how will you answer to our customer base and the media, and rebuild trust?</td>
</tr>
<tr>
<td>General counsel</td>
<td>Can you fully articulate the legal risks and obligations after a cyber incident?</td>
</tr>
</tbody>
</table>
A shared responsibility model leads to trust

The way that your organization internalizes customer responsibility is to build it into the DNA of your company. Some brands have created a “Trust Center.” This Trust Center can enable transparent customer experiences, including how and when data can be used or shared. Exposing information about how an organization goes about its information security practices, including secure software development, can break down the knowledge barrier and daunting aspects of security and privacy to increase customer trust.

A few brands have made commitments about how they strive to make their customers’ lives better. These declarations have built, and increased, trust with their customer base – and security and privacy need to make this list.

NORDSTROM

Customer service

amazon

Get it fast

Apple

Lifestyle technology

LEGO

Play for all ages

McDonald’s (M)

Consistency
Corporate culture obsessed with security

Famous clichés like “move fast and break things” are disruptive statements from an earlier era, and no longer good mantras for technology leaders. Racing to market with products and cleaning up the mess later goes against today’s best-practice risk management principles. In this market with complex technical dependencies, buyers, sellers, suppliers, and regulators won’t accept this anymore.

We must assume more responsibility to the public with security policies and controls that put the customer first over our desire to crush the competition.

We must assume more responsibility to the public with security policies and controls that put the customer first over our desire to crush the competition. With so many new cycles of innovation like AI/ML, and increasingly global threat actors, more companies are hiring chief ethics officers to address corporate culture implications to brand equity, and to answer the question: What is our responsibility to the greater good?

We can all grow up if we can recognize that as much as it may be quantifiable, security is a qualitative discipline. Security practitioners have always been valued for their expertise. By taking a top-line attitude, connecting the dots to a much more complete view of security, and with a mantle of ethical priority surrounding everything we do, the CISO, the board, and fellow officers must partner to fulfill our responsibility of empowering the future.
Communicating to be understood

In the cloud, where everything is programmable out to the edge, protecting code becomes the mission. As CISOs and DevSecOps team leaders, our effectiveness in reporting security program performance - especially in terms of application security - has never been more urgent and paramount. Digital transformation compels us to prioritize the security of product lifecycles, and to educate our stakeholders by integrating business objectives into continuous security oversight and reporting.

10-second takeaways

• Shift your talking points to reflect functional business objectives instead of security objectives.
• Embrace defensible instead of obsessing over being “secure.”
• Streamline tools to ensure technology and people are being deployed efficiently and effectively.

“There is no such thing as a completely secure system. If you’re not innovating within your security program, you’re standing still. If you’re standing still, you’re falling behind.”

By Tony Spinelli
CSO, Urban One, Inc.
Board Director, Peapack Bank, Blue Cross Blue Shield
Co-authored by John Hellickson
Field CISO, Coalfire
Message sent is not message received

For non-technical stakeholders, ROI calculations and cyber performance metrics have been murky at best for decades. However, with a shifting economy pushing us into a cloud-dominant computing environment, we need to show our fellow officers, directors, team leaders, employees, and customers how to think about measuring what we do.

Secure versus defensible

We can build a defensible application. But can we build one without a single point of failure? Not likely. Security needs to be reported on as a race we run every day to beat the bad actors, who are working feverishly to break into our system while avoiding detection. Two critical measures to capture defensible positions in reporting are:

Dwell time reduction

This concept helps to remove any unrealistic expectation that security is infallible. Boards can be conditioned to judge security performance on how quickly we identify and contain threats. Prioritize threats and vulnerabilities that will matter to the board, then figure out dwell time reduction tactics and the simplest ways to measure and express them.

Failsafe measures

These contingencies and practices are designed to respond to and minimize damage from a specific threat unique to the enterprise. This will get all leadership involved in translating resources into security posture and connecting simple and straightforward metrics to each priority element.
Zero trust

Zero trust is a network architecture. Cyber teams need to work with developers, starting with the first scrum, to build failsafe measures into every app, especially those that come into human contact. Zero (or at least minimal) trust is also a management philosophy that can be illustrated and understood by all stakeholders in a world without perimeters. Everyone, from the leadership team to the end user, can comprehend the strict default position that no device or touchpoint can be trusted, even if connected to the corporate network, or even if previously verified.

Tool baggage

The “buy tech/fix problem” mentality has been around for decades. With hybrid cloud environments and questionably secure code thrust out to the edge of networks, this mentality is dangerous for security leaders.

In direct conflict with the perpetual motion of cloud security, tool baggage exacerbates the point-in-time mentality that we need to get away from. CISOs fighting for their share of budget that later appears on a spreadsheet of capital expenses is not a productive way to implement a continuous integration mentality into your reporting.

Having a multitude of products means you’re going to need a multitude of people to know them and gain their utility. Again, expense line items of security product purchases and more headcount to support those expenditures is not the way you want to manage your program, report on it, or to have your own performance judged.

78% of enterprise CISOs have 16 or more tools in their cybersecurity vendor portfolio.

Gartner
Top tips for CISOs reporting to the board

1. **Break the mold**: Security is not point-in-time and requires continuous metrics.

2. **Frame the risks**: Connect enterprise products with the code that creates them to show how security protects each product along its unique journey to the customer.

3. **Executive dashboards**: Keep it simple with minimal factors to track, and stay away from the highly technical. Build a risk register with factors determined by the risk priorities that have the greatest impact on your organization.

4. **Align with business unit leaders individually**: Learn their strategy, align security into their challenges, and get their support before stepping into the boardroom itself.

5. **Build capability**: Include in your reporting narratives about DevSecOps team integration, your philosophy on enterprise risk priorities, and how you can compare your security operations with peers, with competitors, and within regulatory frameworks.

6. **Build support**: Include processes correlated to costs and revenues that clearly show business impact.

This is a journey, one of technology and methodology adoption, and of cultural change. It all boils down to keeping software secure. It sounds simple, but this is a profound change from the way boards of directors have traditionally viewed security: Criminals breach inside a system and steal data. Now the very lifeblood of our enterprise – the product code – is outside the disappearing perimeter, exposed everywhere.

“*CISOs have to be right on every decision, 24/7. The bad guy only has to be right once.*"
The secure customer experience

Boards and C-suites are more attuned to enterprise security risk than ever before. So are vendors, suppliers, and customers. It’s about time. We as security leaders have been talking about using “security as a marketing tool” for years, but the time for talk is officially over.

Today, everyone is cybercrime aware. If they’re not demanding it already, just about every B2B and B2C customer will soon come to expect upfront assurance from their providers that security is 100% present and accounted for. This goes as well for vendors, suppliers, partners, regulators, courts, utilities, governments, countries – everyone.

10-second takeaways

• Incorporate security and trust into messaging alongside features and specifications.

• Understand that competitive differentiation is a team sport that requires knowing how to talk about being secure internally and externally.

• Ensure customers know that you, and your supply chain, are secure and be able to back that up with certifications and proof points if asked.

“The goal here is to instill in all your constituents that security is at the core of every relationship and baked into your company’s DNA.”

By Gail Coury
CISO and Senior Vice President, F5

Co-authored by Nate Demuth
Senior Director, Cloud Services, Coalfire
Security as a revenue enabler

This is part of the value discussion that has evolved over time, where security and the currency of trust can be looked upon as marketable business processes that have measurable returns on investment. As the interface between customer and company becomes more digitized, customers want to trust the company’s entire digital landscape. They need to know their identity and data are protected, business continuity is assured, and that the user interface is a security comfort zone where buyer and seller can streamline their work together with minimal frustration.

The value proposition is clear: Protect customers’ identities and make sure they know about it. Through use of our technology, organizations are able to deliver a more frictionless customer experience with easy but secure authentication, logins, payments, and shopping cart and session continuity. Even if their data is protected, customers value their time, which if squandered and disrespected becomes yet another trust issue. Customers want security, and they also want streamlined ease of use.

Telling your security story: The most effective GTM tactics

- In-person discussions/workshops as part of purchase process
- Access to compliance reports
- Maturity score/benchmark (e.g., against frameworks, industry peers, etc.)
- Pen test results
- Customer-facing collateral providing high-level overview of security approach
- Vendor security assessments provided by partners/service providers
- Customer-facing collateral providing detailed technical/security blueprints
- Security rating by third party (e.g., BitSight, Security Scorecard, etc.)
Pathways to competitive differentiation

Look in the mirror

Security professionals have been viewed by our coworkers as dogmatic tool pushers and rule enforcers for far too long. This perception likely stems from the fact that security leaders have traditionally not been as closely aligned to the business as other leadership roles. It’s time to grow up and out of this image and contribute business perspective if we want our organization’s cyber effectiveness to mature and keep up.

- Confirm that leaders understand risk-based problems and solutions and know how to discuss security within the context of their functional areas.

Evangelize executives

To get everyone thinking about security as a marketing tool and revenue driver, start by initiating conversations with your board and executive leaders. Instead of an expensive bad cop that most people in the company tend to avoid (especially developers), your department becomes the source; the one with the answers for how to empower business and security together.

- Develop the language and communication skills that make it easy for every employee to tell the story of a cyber-aware brand that others aspire to be.

Have customer conversations

As part of any pitch or proposal, include an element that shows off your compliance certifications (e.g., PCI, ISO, etc.), and educates prospective customers about how you will develop and apply security controls and contingencies on their behalf over time. People of all technical aptitudes need a helping hand to understand what protections are needed and are in place, and how to bring those messages back to their own customers and internal departments.

- Integrate communications between security and the customer at the initial engagement and in the business development phase. Offer CISO-to-CISO conversations to start the dialogue around security thought leadership.
Security frameworks have evolved like wildfire in recent years. Markets and marketers barely knew what they were until the proliferation of GDPR, CCPA, CMMC, ISO, and dozens of others. They are quickly embedding into the collective consciousness, and even the least technical among us understand their value as security seals of approval.

- Customers may say they are not willing to pay extra for an accreditation acronym stamp of approval, but the absence of third-party certifications can nevertheless become a deal breaker. Understand the value and differentiation that results from the certifications, and share that with your customers.

**Frameworks – the new seals of approval**

**Secure the code**

With digital transformation, security is more important for ensuring brand integrity and customer trust. It’s time for us technologists to become true business leaders. Help developers by sharing security responsibilities and doing the right thing by integrating secure code from the get-go.

- Model threats together in the first agile team meeting. Reward security excellence in development lifecycles. Educate executives, employees, vendors, suppliers, and customers that secure product development is out front, and that development security is baked in from the first scrum to the end of the product lifecycle. Explain and drive this home with your customers’ security and marketing teams.

**Be the enabler**

Have conversations with your heads of marketing so they, in turn, can integrate security messaging into their demand generation efforts and relay those value propositions to customers. For virtually all commercial enterprises, there’s going to be a lot more exposure along the secure product lifecycle, with lots more applications scaling up and down in the cloud or on a SaaS platform.

- Provide everyone in the organization with the knowledge and understanding of risk management and security controls to help them incorporate that into business decisions.

**Walk the talk**

From now on, in every department and business unit, always ask: *How are we integrating security into our daily work activities, and how will it improve the customer experience?* Then you can market your organization as one that cares about security, and as one that is fundamentally mature in its cyber mission and culture.
Conclusion

Competition and the rapid adoption of cloud technologies are driving organizations to build software in a new and distinctly different manner. Standing on the shoulders of the Agile Manifesto, this emerging methodology can be defined in simplest terms as security and development coming together as one.

This is the final shift left, where there is no longer any daylight between spirited coders striking out on a new project and risk-savvy cyber pros, together in the same scrum on day one. DevSecOps now more broadly describes the traditional development process. It’s not replacing agile, but it’s interesting that the word “security” was never mentioned in that original manifesto from 20 years ago.

This report has brought together some of the best minds in IT – cybersecurity in particular. Most of them were there back then, pioneering the origins of AppSec and what has evolved today into best-practice cloud security management. What they’ve brought forth here in this report maps out the next generational change in securing the CI/CD pipeline.

Continuous integration and continuous development draw heavily on automation and technology configurations to increase the pace of software delivery while lowering the potential for cybersecurity risk.

Adoption of this approach is a business imperative – the traditional ways of building software are not able to keep up with business demands and inject far too many software vulnerabilities into production.

We appreciate our CAB members for their wisdom on the new security paradigm, and for their unique experience that sets the tone for this once-in-a-generation opportunity. Thanks for showing us where the puck is going.
Coalfire co-authors

Patrick Kehoe
Chief Marketing and Strategy Officer
30 years in technology/go-to-market leadership roles with 10+ years of cloud and cybersecurity experience

Caitlin Johanson
Director, Application Security Services
13+ years of security and engineering experience

Mike Eisenberg
Vice President, Strategy, Privacy, and Risk
Former Global CISO with 35+ years of security experience

Adam Kerns
Managing Principal, Cloud Engineering
18+ years of security and engineering experience

Matt Klein
Field CISO
Former CISO with 25+ years of security experience

John Hellickson
Field CISO
Former Global CISO with 30 years of security and infrastructure experience

Nate Demuth
Senior Director, Cloud Services
10 years of security and consulting experience
About Coalfire

The world’s leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success.

Navigate the smartest path to your DevSecOps transformation.

877-224-8077 | Coalfire.com