WIZ

Building a strategic cloud security program

Accelerating your organization with cross-functional security.

Table of Contents:

Security is a C-level problem: Making the case for cloud security

Cloud-based operations continue to transform the way organizations operate, and for good reason. The cloud is easy to use, relatively safe, and more reliable than traditional computing, but it also comes with its own unique challenges and risks. Multi-tenant environments create a more complicated network of cross-app compromises, an internet-based infrastructure introduces new paths for bad actors to exploit, and a decentralized cloud architecture makes organizations more vulnerable to exploits and breaches.

For some companies, security and cloud security may be treated as one and the same. But to effectively reduce cloud costs, improve ease of audits, and reduce the risk of exposing sensitive digital assets, cloud-based organizations have to rewrite their security playbook. In the face of these changes, lines of business that rely on the cloud need to explicitly agree to accept risk implications and comply with security policies and best practices.

At a business level, this prioritization means avoiding costly regulatory fees, preventing operational disruptions, securing intellectual property, and maintaining reliable brand fidelity in the eyes of your customers. Security is everyone's responsibility, and when working to get other C-level executives to adopt a culture of cloud security, it's important to frame that culture as a collaborative effort. Without cross-functional buy-in on cloud security, a cloud migration can end up slowing your organization's growth as you attempt to fix problems after they arise instead of preparing for them.

The only way to prioritize cloud security is when other teams are helping work toward the same goals. Help your C-level colleagues consider how security is a business enabler, rather than a cost center. Discuss the implications of not having a security team. Which metrics should be tracked (and which should be shared)? Addressing these together will help build an organization that prioritizes security as a shared commitment that drives the business forward.

Quotations that appear throughout this book have been taken from a workshop conducted with global security leaders from across several industries including entertainment, finance, technology, travel, and more. They have been edited for brevity and anonymized to protect the organizations' proprietary information.

How to prioritize cloud security with your C-Suite colleagues

Building a culture of cloud security doesn't happen overnight. You can accelerate the process by focusing on a few key areas of your security program's relationship to the rest of the organization. At the heart of this process is communication, and using the following steps can help you get buy-in from other teams and leaders across the company.

Part 1: Outlining your organization's unique cloud risks

Many organizations don't consciously or proactively reset their approach to risk when migrating to the cloud. But this reset is vital because migrating can immediately lead to new vulnerability exposure. The potential exposures that come from multi-tenant environments or connecting your infrastructure to the internet are not problems that an IT team has to worry about.
Systems may have their own disadvantages, but a benefit is that security teams have the peace of mind knowing that all of their data is safe from outside agents.

While cloud-based organizations are more scalable and agile, moving to the cloud also exposes their data to new threats — such as cyber attacks and exploits in their cloud provider's infrastructure — that are beyond their control. Since these risk factors are fairly universal across cloud providers, cloud-based companies also share consistent cloud risk profiles. These profiles include concerns about damage to their company reputation, legal issues, or contractual obligations. While these profiles may be consistent, risk tolerance differs drastically from company to company and industry to industry. As security threats continue to evolve and affect new industries in new ways, understanding how those threats impact your business needs is vital.

The first step in the conversation around cloud risks for your organization is breaking down your unique risk appetite and risk tolerance to build your cloud risk profile. By painting a clear picture of core business drivers and your team's speed to market demands, you'll be able to understand how comfortable the business is with deviating from risk standards to meet its goals. This process also gives you a sense of which areas of your security strategy need to be prioritized to support those objectives.

> **You have to quantify and qualify operational risk exposure in the language of your business to ensure your CEO understands.**

Developing and presenting a comprehensive risk profile to showcase potential threats, how they'll impact your organization, how likely they are to occur, and what tools or strategies you'll need to protect against them gives other leaders an easy story to follow so you can promote a cloud security culture. But risks don't stop at protection.

During this part of the conversation, be sure to raise the need for a recovery plan, as well as a protection plan. When 83% of companies inevitably experience a data breach, and breaches for U.S. companies cost double that of the global average ($9.44M versus $4.35M), the security conversation has to extend well beyond a first line of defense.

Using more stringent regulations to drive your cloud security needs

Regulatory oversight has long been an accepted part of sectors like financial services or healthcare. But regulations change, and industries that have not been heavily regulated in the past are now under increased scrutiny when it comes to data security. It means that teams have to be more vigilant. It also opens the door to broader conversations about your security posture.

> **If you have executive management and a board with regulatory overhead, the more regulation spreads into your business, it'll be more important for the security team to get involved.**

Additional regulations require new discussions around risk. While your leadership is focused on innovation and new projects, regulatory overhead provides you with new guardrails to plan and execute security priorities. As regulations change, your CEO will have more reasons to get involved in understanding the scope of the changes and their impact on your organization.

Addressing risk ownership and identifying security partners

With a clearer understanding of the risks your organization is taking on, you can work to establish who owns your risk management. Though security is the main driver, it's important to remind other teams that everyone must have a hand in keeping your cloud secure in their daily work. This differs from an on-premises operating model, where security can have full control to secure new applications being developed.

For example, if one team begins developing a new app in your cloud environment, the developers building the app must share the responsibility for risks that app may introduce. Ensuring that security is a shared responsibility will involve providing tools and training for teams to efficiently address cloud risk and deciding which leaders are charged with security controls. As you continue higher level strategic conversations around security with your C-level colleagues, consider what resources you'll need to equip your cross-team partners.

Part 2: Proving cloud security's return on investment

Using regulations to start the conversation about cloud risks and needs is helpful, but it's also important to frame cloud security as a driving, positive force rather than a solution to a problem. To reposition your cloud security initiatives as business drivers, it's crucial to tie your goals to the organization's overall business goals. Compliance (and avoiding regulatory fines) is certainly one goal, but consider how the business is generating revenue and how you're going to be an enabler for its success.

> **It's about telling other business leaders 'I'm not here to slow you down.' When innovation is the lifeblood of your company, you have to make it clear that you're going to enable that and sustain your growth pace by making the business more resilient.**

Cloud security drives the same business goals as cloud computing

Prioritizing cloud security in your organization's business plan should be at the same priority level as the cloud in general: your team can be more agile, more resilient, and help reduce overall IT costs. Much like your initial cloud migration, moving from capital expenses to operating expenses creates a huge shift in cost early in your cloud security transition.

But scaling your organization with a more collaborative, secure-by-design development process means that you can unblock new technologies to accelerate the business. The security program, in turn, pays for itself by making the business more efficient. To justify the initial cost shift, work with your CEO to determine exactly what resources you'll need to reach this degree of efficiency.

An industry-leading security plan requires an industry-leading team

To set your plan up for success, you'll need to assess what skills and which people you'll need on your security team. Recruiting the best engineering talent is only possible when you're using the latest technologies. Understand exactly which technologies best align with your industry and what processes you'll need to use them effectively. These improvements mean that you can more easily detect and measure defects sooner in the development process (and more importantly, prior to production environments) to create a culture where security is proactive.

With a better-equipped, more efficient security team, you can securely develop new features, protect your existing customers and IPs, and build a self-sustaining security ecosystem that drives the business forward.

A more resilient business is a more successful one

Your cloud environment may be exposed to more threats than a traditional, on-premises environment, but it doesn't have to mean it's less secure. Cloud computing is often more resilient because of cloud providers' storage redundancies, and the same can be said for a leading cloud security strategy.

A robust cloud security strategy helps prevent downtime across the company. If a new app is hacked due to a missed vulnerability, that may delay production or release dates and impact your organization's bottom line. With the right tools and processes in place, your team can reduce business disruptions caused by vulnerabilities and keep work across the organization running smoothly.

A safety net for your organization's most important assets

At a literal level, cloud security protects your IT infrastructure, but by protecting your cloud environment cloud security is also guarding your company's value. Your cloud infrastructure houses your intellectual property — your competitive advantage — and a secure environment ensures your business's secrets stay secret.

Secure operations also ensure that regulatory compliance is part of the conversation before it becomes an issue. By baking compliance early into the development and deployment pipelines, you can avoid regulatory fines.

Cloud security also has the blessing and curse of being a behind-the-scenes function. A well-executed security strategy helps protect your brand image. As we discussed above, it's not a matter of if a breach will happen, but when. By educating your teams on proper security steps, you can minimize the scale of a breach, remediate, and ensure the impact to your business's wallet and brand are minimal.

Part 3: Demonstrating measurable progress of program growth

As with any other high-functioning part of an organization, being able to track, measure, and optimize your team's performance is essential to its success. Introducing metrics is simply the start of using them as a tool to aid conversations with other executives.

"We have to give board members and other executives metrics that are credible, but not overly technical," says Drew Simonis, CISO at Juniper Networks. This creates an environment where everyone can comfortably weigh in on security's business impact. Since team members across the organization have a variety of (and sometimes competing) priorities, they'll also have varying sentiments toward different metrics. Creating a system to reliably measure the impact of your cloud security program and prioritize metrics that resonate across your organization builds team-wide trust.

Priority 1: Meeting NIST standards

Since production defects are much more expensive to manage than those that occur earlier in the software development lifecycle, it's important to shrink the time between surfacing an issue and acting on it. Adhering to NIST standards, including the Cybersecurity Framework (CSF) and using the Secure Software Development Framework (SSDF) should be your top priority as a business-focused security team. Since these frameworks already exist, you can use the SSDF as a threshold for a successful security program. The nontechnical language of the CSF and SSDF also make them helpful tools for communicating your success to other leaders.

CSF sets the bar for your organization's security standard, which means you can use it as a springboard for developing KPIs with your CEO and other leaders. The five pieces of the framework—identify, protect, detect, respond, and recover—outline how your team responds to cybersecurity risks. By establishing which elements of your organization's operations are mission critical (such as the ability to collect payments for an eCommerce platform) in the "Identify" stage, you set a baseline for uptime metrics and can sift through noise to find exactly which steps you have to take to meet that goal.

Priority 2: Retaining low Mean Time to Detect and Respond (MTTD/MTTR)

Setting detection and response metrics can also help demonstrate exactly how a cloud security function is safeguarding the organization. By monitoring MTTD and MTTR, you can quantify how and where you create efficiencies that support key business projects. For example, you can measure how much time it takes to surface an issue to a developer and how quickly they can take action on the root cause of an issue to accelerate project development.

Priority 3: Limiting security risks as your cloud environment scales

Growth is exciting, but maintaining and scaling existing processes alongside that growth introduces new challenges. Tracking how your security program adapts to a growing cloud environment can help you better understand what resources you need where and how you can better manage issues at scale. Daily metrics related to scaling your security program may include incident volume (both for incidents and near incidents) and ticket volume. Is your team closing out tickets, or is your technical debt outpacing your remediation speed?

At a more strategic level, you can track your overall volume of security issues with a goal of keeping that number consistent (or, ideally, decreasing it over time) as your environment grows. One way you can decrease that number is by focusing your efforts on addressing entire classes of issues. By identifying and fixing root causes rather than individual, potentially recurring issues, you can get ahead of your technical debt and grow securely.

Priority 4: Improving adoption of your cloud security toolkit

More tactical measurements of success like those outlined above are your organization's key security drivers, but as you meet them, you can also work with your team to set aspirational goals to nurture your cloud security culture. A strong leading indicator of a healthy security program is your platform's Monthly Active Users (MAU).

> **If we saw a major drop-off in usage from our development teams, that could be a sign that we're burning them out or they're finding less value from our security information. You can use that information to find a solution.**

By evaluating platform usage, you and your executive team can determine whether people are using the tools they have to make change. This may include not only your security team, but also developers and business teams to understand how engaged the company is with your security program. If everyone in the organization is accountable for security, everyone should also be using the security resources they have available. If people aren't using those resources, you can work together on a plan to encourage adoption across the organization.

Part 4: Establishing a system for continuous improvement

When IT, product, operations, and other cross-functional teams are working closely together to create a tight feedback loop, you can ensure you can meet business needs without compromising on security risks.

> **If we hire this engineering team, and we're able to comply with these requirements for this EU compliance framework, we'll be able to unlock millions of dollars worth of opportunities.**

This collaboration may look like focusing new security projects on unlocking new regions for business operations by meeting new, localized security standards. Creating these collaborative projects is easier said than done. To get started, take a longer look at the high level goals of your cloud security program.

Aligning on your security program's goals

Setting program goals before diving into individual projects ensures your daily security work is all working toward consistent objectives. Program goals are tied directly to finding, addressing, and protecting against risks across your business. Working toward gaining complete visibility of your cloud environment, for example, can give your teams more time to address issues rather than search for them.

These goals aren't meant to be met overnight. Ongoing improvements to managing vulnerabilities and securing your data all contribute to an evolving culture of security. Small wins add up, and you can work toward shifting left gradually to build security into the foundation of your development pipeline and ultimately, your entire business.

You know what you need to measure. You have your strategic goals set. Let's explore how you can build a process for completing the day-to-day work that will help you meet those goals by reviewing what a RACI (responsible, accountable, consulted, and informed) matrix might look like for your next big project.

Designing a RACI matrix for your next cloud security project

Building a clear process to meet your project goals helps establish an unobstructed path to production for new initiatives. By preparing sooner and understanding which parties are responsible earlier in the development process, you can create the most secure route for your business.
At the outset of a new initiative, ask yourself and your collaborators what you'll need to start:

- Which teams should be responsible and accountable for the overall project?
- What committees need to be formed to keep communication open?
- Which stakeholders need to be consulted or informed to be kept in the loop? This will also include determining how involved leaders will be with day-to-day project management.

With your stakeholders set, consider which meetings need to be scheduled, which organizational processes need to be followed, and which tools should be put in place to design a successful, secure project. The tools you choose should help reinforce your collaborative approach to security by supporting both practitioners in their project work and providing an executive view that leaders can use to guide future decisions. Using the techniques discussed above in combination with the proper toolkit can inform the "why" of new projects and help facilitate an organization committed to growth and innovation. It also builds those developments on a foundation of trust and security.

This is especially important in recognizing everyone's individual impact on an organization's security posture. By 2025, human error will be responsible for over half of significant cyber incidents, but it should be made clear that this burden isn't any one individual's fault. Using proper systems and processes to collaborate more effectively across your company helps center the human experience of navigating the complexities of cloud security as a team. A united front better prepares your entire organization to grow quickly, intentionally, and securely.

Another key partner for building a strong security program is your governance, risk, and compliance (GRC) team. Working with your GRC team is mutually beneficial because analysts rarely have the right tools to fix compliance-related issues. They'll look to your team and the product team to prioritize a secure by design approach to development. You can work with your GRC team to look at security and compliance, tie their goals to business objectives, and attach dollars to security initiatives to strengthen the case for senior leadership.

Summary

Creating a culture of cloud security means your organization celebrates your successes and prioritizes meeting challenges for the collective good of the organization. Building this culture starts with helping your C-level colleagues understand the business drivers (or blockers) associated with cloud security, discussing risks, and measuring performance together, so that you can work together to create a more efficient, more secure, and more successful organization.

Appendix

Topic	Key questions to ask	Goal

Part 1: Outlining your organization's unique cloud risks	• What are our core business drivers?
	• What are our speed-to-market demands?
	• What regulations do we have to adhere to?
	• What potential threats do we face?
	  • What is our protection plan against these threats?
	  • What is our recovery plan?
	• Who owns cloud security?
	  • How is the responsibility of security shared across your organization?
		Understand your organization's risk appetite and risk tolerance to build and evaluate your specific risks, what it will take to protect yourself from them, and who will manage that defense.

Topic	Key questions to ask	Goal

Part 2: Proving the return on investment of cloud security	• How does improving security help generate revenue?
	  • How does improving resilience drive innovation?
	  • How does having a resilient security program reduce costs?
	  • How does improving agility drive innovation?
	• How does improving security reduce IT costs?
	• How does a secure by design development cycle help accelerate business growth?
	• What hires will need to be made to scale your security program?
	• How does protecting your intellectual property and brand help growth?
		Create a clear connection between improved cloud security and faster business growth with reduced costs.

Part 3: Demonstrating measurable progress of program growth	• What are your organization's most important metrics?
	• What security metrics will help demonstrate cloud security's contribution to the overall business?
	  • Ex: Use NIST standards like SSDF and CSF to set a baseline for your cloud security needs.
	  • Ex: Use MTTD/MTTR to communicate how your team keeps the organization scaling securely.
	• What can you do to limit risks while your organization grows?
	• What aspirational metrics can you set to create growth goals for your team?
	  • Ex: Review Monthly Active Users of your cloud security platform to get a pulse check on who in the organization is keeping up with your security goals.
		Establish clear, measurable goals for your cloud security team that are easy for nontechnical team members to understand, monitor, and review so you can better quantify security's impact.

Topic	Key questions to ask	Goal

Part 4: Establishing a system for continuous improvement	• What other teams are working on collaborative programs?
	  • How do these new projects help support multiple business initiatives?
	• What are your goals for your security program?
	• What projects do you have to take on to achieve those goals?
	• Who is included in the RACI matrix for your cross-department project?
	  • Which teams should be responsible and accountable for the overall project?
	  • What committees need to be formed to keep communication open?
	  • Which stakeholders need to be consulted or informed to be kept in the loop? This will also include determining how involved leaders will be with day-to-day project management.
		Design a system for actively collaborating with other teams to foster a cross-departmental investment in your cloud security program and projects.

About Wiz

Led by an experienced and visionary team, we're on a mission to help organizations create secure cloud environments that accelerate their businesses. By creating a normalizing layer between cloud environments, our platform enables organizations to rapidly identify and remove critical risks.