TAG

EMPOWERING LEADERSHIP FOR SECURE INNOVATION: INTEGRATING SECURITY BY DESIGN IN CORPORATE CULTURE

DR. EDWARD AMOROSO,
CHIEF EXECUTIVE OFFICER, TAG

SecurityCompass
THE SECURITY BY DESIGN COMPANY

EMPOWERING LEADERSHIP FOR SECURE INNOVATION: INTEGRATING SECURITY BY DESIGN IN CORPORATE CULTURE

EDWARD AMOROSO, CEO, TAG

GETTING STARTED WITH SECURITY BY DESIGN

Software developers and cybersecurity practitioners interested in engaging in a new program of Security by Design are encouraged to keep in mind several design principles that we've found to be effective in practice. The first principle involves recognition that modern security leaders have considerable challenges that must be addressed. This implies that process improvement is focused on solving real problems.

The second principle is that Security by Design is best adopted and maintained as a combined executive and corporate initiative. That is, the approach is not to be done in isolation but rather through an integrated program of executive sponsorship and developer adoption. This includes the provision of the proper resources and support so that the design approach can be translated into actual security preventive actions.

A third principle worth mentioning is that the roles and responsibilities for achieving Security by Design should be clearly identified. Leadership, in particular, should be tasked with driving a culture that supports doing things correctly from the beginning, rather than waiting for problems and responding afterward. Such emphasis on culture ensures that involved developers and security team members will make good decisions in practice.

ESTABLISH EXECUTIVE ALIGNMENT

As suggested above, leadership must set the tone for Security by Design. The 2023 Secure by Design paper by CISA and others acknowledges that it must be both an executive and a company-wide initiative. Full buy-in at the senior executive level is crucial, ensuring that even if initiated by middle managers and application security leaders, they receive full senior executive support.

This means Security by Design requires alignment throughout the organization, from setting correct priorities and incentives at the executive level to implementation and follow-through at the operational level. This alignment should not dictate specific development decisions, like the choice of threat modeling tools or AI assistants but should ensure that development team priorities are in line with the organization's overall mission and goals.

ENSURING FULL GRASSROOTS ACCEPTANCE

While executive buy-in is critical to a culture of Security by Design, the organizational focus must always be on the software developers. Introducing this new development paradigm involves a significant change in the lifecycle approach, and it is thus often met with resistance (as with any type of substantive change). Developers may question its applicability or impact on their workflow.

For example, if an executive explained to an entire company the goal to integrate and implement Security by Design *today*, then this will almost certainly create immediate resistance. Developers might say things like, "Well, I don't know if it's going to work for us." Or they might say, "I don't understand what this means to me or how it affects my workflow." These are common responses to any executive demand for change.

To address these concerns, teams should implement proper cultural change, including basic practices such as running pilots, finding the right teams to adopt the technology first, encouraging teams to adopt new practices, and embedding Security by Design into the performance review and incentive process. These commonsense steps will help to ease an organization into the more preventive approach for software security.

The overall approach may also be enhanced by recruiting developers who are passionate about security and are willing to be trained as security champions so that there are embedded security-trained developers within the working groups who are responsible and accountable for delivering secure code. This serves to create cultural train from within the software development community.

THE IMPORTANCE OF CULTURE IN SECURITY BY DESIGN

Security by design involves integrating security from the very beginning of the development process. But one of the most critical aspects of driving this approach involves the culture that embraces this attention, and that is perhaps the hardest part of building in security by design because it references people, processes, and their interactions during development.

The first step in establishing a strong culture of Security by Design involves convincing developers to make security a key requirement. This is not to say there aren't security aware and responsible developers, but when it comes to their job function, they might not be compensated or incented to focus on security. Tools and co-pilots will help, but mindsets and incentives must shift.

We've consulted Security Compass, experts in Security by Design and they agree that it's common to encounter developers who are wholly aligned to the production of value for end customers, but less so on ensuring security. They focus on shipping features, fixing defects, and other tasks that are directly related to the customer's needs. And while security might be important to an individual developer, it's too often not seen as their particular job responsibility.

Referencing the CISA paper once again, there is motivation to provide security as a default feature of products (and the software and applications within them) rather than as a luxury feature. So, with this proposed shift in customer expectation for security, there's an emerging trend to shift the development culture to consider security as a valuable product feature as well.

SUPPORTING DEVELOPERS ON SECURITY

At TAG, we have observed that in many companies, developers will say that it's the CISO-led team's responsibility, usually in an application security group, to ensure the security of code. The problem, obviously, is that the cybersecurity team is not the group developing and writing code. Furthermore, it is not uncommon for application security teams to have only a surface understanding of the actual software development process.

Security Compass's survey revealed that 74% of developers engage with security after the design phase. Responders claimed to not think much about security in the design phase. They don't have the right tools, they're building software too quickly, and they don't have time to slow down and think about security. They are also not traditionally trained in security and will usually see it as slowing down their coding.

When the Security Compass team explains Security by Design, they emphasize providing developers with the required security support and training they need on methods such as threat modeling, secure coding, and other proactive means. The goal is to drive integration of security into the planning and coding phases of the DevOps lifecycle. At TAG we believe that this might be the secret to significantly reducing the intensity of breaches.

ROLE OF SECURITY EDUCATION

Rather than viewing security as the sole responsibility of some different department, software teams must learn to embrace security, starting with the design process. This shift in emphasis requires that excellent security educational resources be available to develop security skills and to establish grassroots support across all aspects of the software lifecycle teams. Executives should ensure support for such objectives.

The Security Compass team recommends starting the Security by Design journey with an intense focus on creating and maintaining world-class cybersecurity education for teams and their members. We agree wholeheartedly with this approach. In fact, this can include in-house or external support, but education is an essential component of establishing a culture of Security by Design.

The next step is to embed this security knowledge within the development teams. One way of doing this involves establishing security champions or security coaches into the development team and making them the steward for security in that team. Their job is to localize and tailor the learnings and best practices developed across the organization. With background and training in development and then a specialized focus on security, they will have the right empathy and understanding for the day-to-day concerns of the development organization.

SECURITY AS PRODUCT QUALITY

A key question for developers is whether they have sufficient confidence in their software. Think about the pride developers have in functional and elegant code. Now, what if they could also build up their pride in coding securely? What would happen if a typical developer could be willing to discuss with a compliance regulator or external auditor the specific preventive design steps that were taken to integrate security into the software?

The good news is that this trend is changing for the better. There are white papers being put out in countries such as the United States, Australia, Canada, the UK, and many other countries around the world about shifting the balance toward security by design and more preventive approaches to software security. The emergence of artificial intelligence co-pilot tools is consistent with this shift left toward creating better software from the start.

CREATING IMPROVED SOFTWARE

Are there other events that motivate developers to develop functionally as well as securely? A recent US Executive Order, for example, discussed improving the nation's cybersecurity and specifically addressed software supply chain through use of tools and constructs such as software bill of materials (SBOM). This method involves automated development of a list of open-source components that the software includes so that users know what they need to patch and where there might be inherent vulnerabilities.

But that executive order also created and helped to spur the NIST secure software development framework, which is a comprehensive approach to addressing security in the SDLC. And this is especially welcome because for one reason or the other, the software community hasn't had good standards for security by design considerations.

The implications for software by design in different industry verticals is encouraging. For example, the US Food and Drug Administration (FDA) could begin requiring threat models in pre-market submissions for medical devices, the payment card industry (PCI) could demand security by design as a mandatory strategy for software, and this can continue across all type of critical sectors.

An impact of all this is that there are additional external factors that can influence the developer organization's motivations and mindset. Software companies must reflect on their obligations to these external stakeholders that make security a requirement and that contribute to the case for security by design.

VALUE PROPOSITION FOR SECURITY BY DESIGN

Ultimately, the goal is to establish a clear value proposition for each stakeholder in the company regarding Security by Design. And this value proposition is rooted in changes around how developers work today, with the goal of finding ways to improve their work and the quality of the software they are producing.

It's key, when establishing a value proposition, that the right stakeholders be included in the process. If the right stakeholders have input to the Security by Design plan, then they can help reduce the likelihood that developers see no problem that needs solving, which can lead to resistance. This can happen at any level of the organization including executives.

The time to implement is also a key consideration. If you tell development teams that they must immediately implement every tenet of Security by Design, then you might introduce serious conflict with requirements promised to customers or included in a delivery schedule. Development teams need time to adjust, so the process should be introduced incrementally.

ADDRESSING SCALE IN SECURITY BY DESIGN

Another common problem that emerges with any change in the development paradigm involves the challenge of scale. For example, a small group of developers might decide to buy into some useful technique such as threat modeling or AI assistance and they might begin to use this in their local software process. This is usually a good decision from a security perspective and will help the quality of their code.

But the scaling of this decision across a large development team usually demands more than just word-of-mouth sharing. Instead, proven methods such as threat modeling must be associated not only with an initiative to scale but must be connected to the deployed platforms that support automation and continuous operation, two features that are absolutely necessary for scale.

This implies that careful consideration must be made into the number of hours required for Security by Design activities, as well as other staff and resource requirements. We've seen proposals for threat modeling, for example, that would introduce hundreds of hours of work to a development process that must deliver in weeks. Obviously, this would cause problems in the time planning for the development team (as well as serious push back on the proposed changes).

PROVING THE VALUE OF SECURITY BY DESIGN

Let's suppose that an important goal is to drive adoption of Security by Design at the grassroots level. The hope is that developers will start to integrate the basic tenets, including methods such as threat modeling or AI support immediately into all aspects of their software development lifecycle, for all the reasons cited above.

A common complaint is that Security by Design is too conceptual and theoretical. And the question emerges: *Can you prove to me that this is worth the time and effort?* Our assessment with Security Compass is that the proof emerges with application. That is, by beginning the process of applying the basic principles, immediate value begins to emerge.

The most common benefits are more secure software with fewer vulnerabilities. Developers immediately begin to see that they are spending less time on manual tasks, because they have introduced automation. In short, the idea here is to prove value by implementing. This does demand that management have the courage, determination, and skills to drive piloting.

ACHIEVING RESULTS WITH SECURITY BY DESIGN

The payoff for Security by Design must be results. Without tangible, measurable improvement, cultural changes and methodologies will quickly fade away. Developers are too busy to be worrying about the latest fad in software security or process improvement. So, achieving results quickly is a mandatory aspect of the process.

The good news is that Security Compass reports having seen amazing results. In one study with a customer, the company saw an 85% reduction in high-risk vulnerabilities. That means lower risk, but it also means less unplanned time for developers. And if there's one thing that every developer knows, it's that unplanned work kills both quality of code and productivity of work.

This implies that one of the core benefits of Security by Design involves knowing what your work is going to be ahead of time. This helps avoid the situation where you are constantly trying to catch up, fixing vulnerabilities when they come up unexpectedly. With Security by Design, you are implementing security controls at a pace you can control.

MOVING FORWARD WITH SECURITY BY DESIGN

Our advice at TAG – and this is consistent with the guidance we've received from Security Compass – is that to start, managers should focus on two primary benefits. First, they should address the quality of work and software process improvements mentioned above. This lies squarely with the developers, and it demands buy-in at the grassroots level and agreement to focus on improvements to culture and enhancements to platforms through automation.

But second, managers must address more hardline issues such as cost. Our experience is that return on investment (ROI) for Security by Design can be significant, and this will be of interest to finance and senior leadership teams. The basis for the involves fewer vulnerabilities driving less reactive and unplanned work. Those hours get focused on building features and delivering benefits to your users.

The cost savings can be enormous. We have seen many companies who claim that a more proactive approach to software security using Security by Design might be the highest ROI component of their entire application security program. This should be intuitive – namely, that avoiding problems up front should save money – and it does.

SECURITY BY DESIGN ACTION PLAN

Let's discuss next steps for your organization. We strongly believe that all software teams should have an action plan in place to drive a Security by Design approach. We assume this would be done in the context of modern DevOps and CI/CD environments, but it can be introduced into any software process paradigm in place.

The action plan should be a multi-step journey, one that involves cultural change. It also needs the active involvement of your people, process, and technology. Work the action plan across all layers of management, up to and including your executives. But recognize that your grassroots developers ultimately will have to buy into the action plan.

At TAG and Security Compass, we are committed to helping your team with your Security by Design objectives. Security Compass has organized its entire company and support for customers around this key concept. Security Compass believes that partnership with their customers can be a critical support element in achieving the goal of Security by Design.

ABOUT TAG

TAG is a trusted research and advisory company that provides insights and recommendations in cybersecurity, artificial intelligence, and climate science to thousands of commercial solution providers and Fortune 500 enterprises. Founded in 2016 and headquartered in New York City, TAG bucks the trend of pay-for-play research by offering unbiased and in-depth guidance, market analysis, project consulting, and personalized content—all from a practitioner perspective.

IMPORTANT INFORMATION ABOUT THIS DOCUMENT

Contributors: Edward Amoroso

Publisher: TAG Infosphere Inc., 45 Broadway, Suite 1250, New York, NY 10006.

Inquiries: Please contact Lester Goodman at lgoodman@tag-cyber.com to discuss this report. You will receive a prompt response.