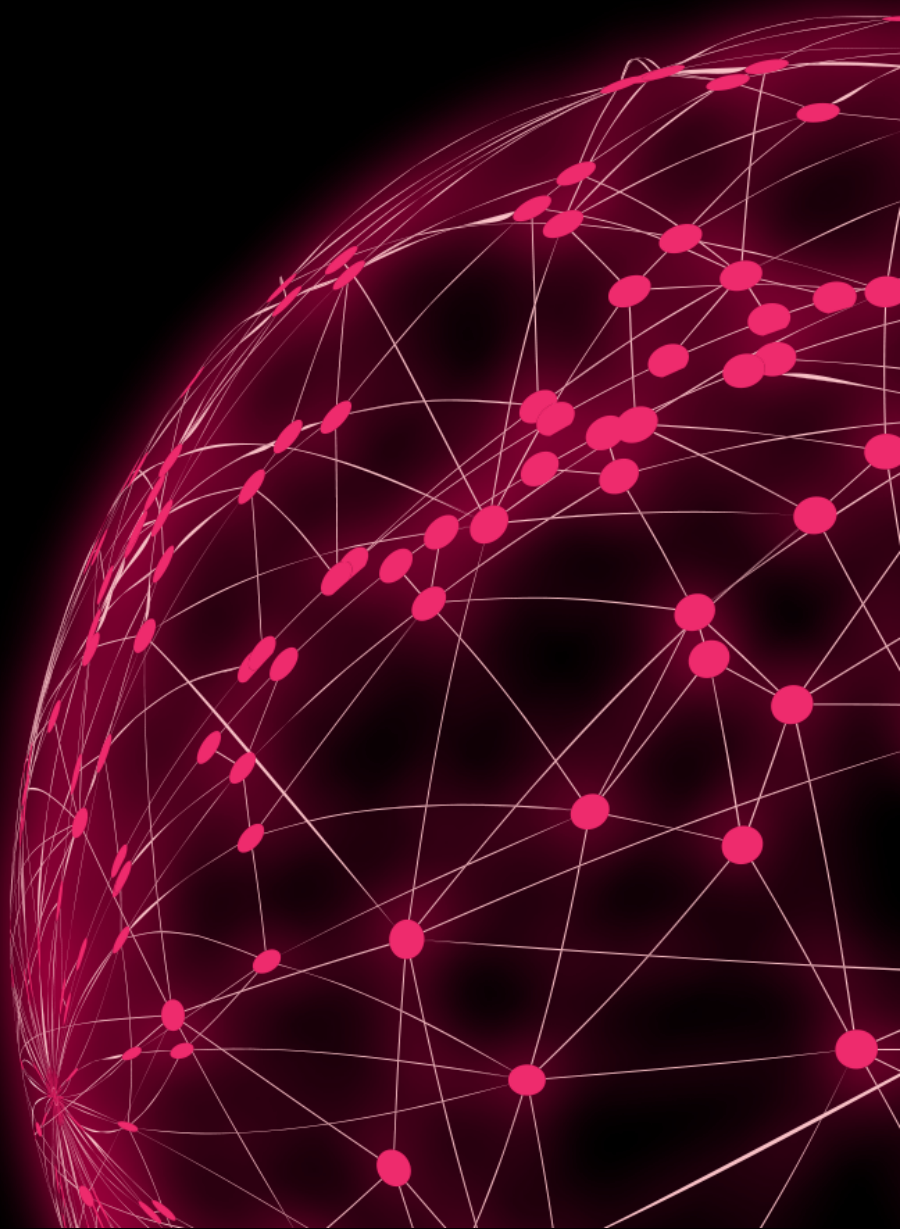
Karamba Security

On the Front Lines with the Product Security Officer: An Inside Perspective



Background

The Product Security Officer is a relatively new role in many manufacturing organizations, especially those that make or use embedded systems in mission critical IoT and edge devices. Definitions and responsibilities vary, but in general the product security officer needs strong technical skills, a deep understanding of security, and the ability to obtain productive cooperation from many different teams in the organization, which do not report directly to him/her. To get a better understanding of this role, how it differs from that of the CISO, and how to create an effective product security program, Karamba Security conducted a series of interviews in April and May 2020.

Representing global leaders in their industries, the interviewees were responsible for product security in their organizations. They shared their opinions on the differences between the CISO and CPSO roles, concerns and solutions sought, as well as best practices that may be of use to others contemplating or undertaking this new role.

The interviewees work in a variety of large, global enterprises, including Fortune 500 and Global 500 companies as well as multinational manufacturers of automation and embedded systems, five of the largest automobile and automotive system manufacturers, global networking firms, and food & beverage manufacturers.

Title and Reporting Relationships

Product security officers have a variety of job titles. Ranging from Global Director of Product Security, to, Chief Software Architect, to Head of Software Development to Product and Solutions Security Officer. However, all of the individuals interviewed for this report have primary responsibility for product security, regardless of their actual title. For purposes of clarity and conciseness, in this report they are called Chief Product Security Officer (CPSO) or Product Security Officer.

The reporting relationships were also diverse, but in most cases the person responsible for product security reported significantly high in the organization; in some cases reporting to the CEO, GM or CTO, and in others to the head of development, VP of solutions and compliance, or head of corporate technology. The fact that the Product Security Officer enjoys an important reporting position in the organization speaks to the importance that product security has achieved in many major manufacturers. In fact, corporations are becoming more focused on product security, because customers' data breach or safety breach can do a lot of damage to the manufacturer's reputation and business.

Product Security Officers' Roles and Responsibilities

The primary responsibilities of the CPSO are similar across industries, with some important vertical-specific nuances. In general, the CPSO and team must ensure security of products, which are in customers' hands, have as few security issues as possible. This starts with architecture and carries through the security-by-design process of coding, threat modeling, testing etc. through to final production. Most CPSOs we interviewed were responsible for governance and policy issues, ensuring compliance with product security baseline requirements and with important regulations. In addition, most mentioned that they feel responsible for making sure that R&D engineers understand the basics of security, and in some cases coordinate activities related to cybersecurity education and training for the development teams.

Q: What is the main challenge of the CPSO role?

> *The biggest challenge is integrating [cybersecurity] into the company culture. Making security a priority, and not an afterthought…trying to build out security by design and incorporating it into the existing product lifecycle."*
>
> Product Security Owner in a major global automotive company

Principal differences between the responsibilities of the CPSO and the CISO/CSO

Interviewees said that the CISO/CSO and IT security teams are responsible for the overall security of the organization, protecting it against active attacks, safeguarding its intellectual property, and ensuring employee cybersecurity education. The CISO focuses primarily on security. The CPSO, in contrast, is tasked with ensuring the security of the product itself, which affects the security of the product end user.

> *The CISO can buy off-the-shelf products and use those to ensure enterprise security. When it comes to product security, we have to incorporate newer technologies with challenging trade-offs, against other attributes (e.g. cost, complexity, performance, safety).”*
>
> Head of Advanced Engineering, European car manufacturer

One of the biggest differences between the roles is that the CPSO responsibility spans not just development but also post-delivery to customers and throughout the lifecycle of the product.

> *The CISO can choose to accept a certain amount of risk, whereas when it comes to products, only the customers can choose to accept the risk. As a Product Security Officer, I am responsible for minimizing their risk.”*
>
> Product and Solutions Security Officer, European Industry 4.0 manufacturing company

Some companies have good communication between the two organizations. This is true for companies where there is some overlap, such as IoT devices that communicate directly with the manufacturer's servers or datacenter. Enterprise security needs to make sure the servers have the correct enterprise security concepts baked in, but product security may need to monitor additional security issues.

> *Despite our large product security team, our company has a small arm within the CISO organization that is responsible for auditing and ensuring the security of our products. They report the audit results to the board of directors every six months. (Additionally,) a small group does independent white hat testing for the product security group."*
>
> Chief Software Architect, Fortune 500 networking company

However, all interviewees mentioned that there is a gap between the two organizations; one person mentioned that there is virtually no relationship between the two, not even collaboration on risk methodology or incident response.

Top issues and challenges faced in ensuring security is built into the product

A majority of the respondents (67%) stated that there are two key types of challenges: one relates to the customer and the other to the product development team.

Customer lack of education about security was mentioned frequently. Large enterprises and government agencies understand the need for security and the value it brings, and they select products according to the level of security they offer. Small organizations sometimes just assume that the product is secure and aren't willing to pay more for security. Some feel that all products are alike, so if they can get a cheaper version from a low-cost vendor, they don't consider the security risks. Many feel that they will not be a target, so education is needed to alert them to the reality of cyber risk.

> *Larger companies have built security into their long-range plans, but many medium-sized and smaller companies don't believe they will be a target. They need education, and we find that ransomware is a useful example. We educate them regarding the steps we take to make sure our product adds to their security."*
>
> Product and Solutions Security Officer, European Industry 4.0 manufacturing company

The product development team often lacks the background to incorporate security by design. This was frequently mentioned by representatives of automotive organizations, where lead times are long and security is viewed as costly (in development effort and software footprint), and more expensive hardware and time are required. When the company uses third-party and supply-chain products or solutions, there is the additional need to ensure that the binaries have been compiled properly and that security has been built in. In addition, several interviewees mentioned the difficulty of making the tradeoff between product features and security constraints.

One company with a well-defined SDLC process, provides engineers with a product security baseline, and tests to ensure they are following the guidelines. Only the General Manager, who has revenue responsibility for the products, has the authority to override a small number of security requirements as long as there is a 3-6-month plan to bring things back in line with the baseline.

A key issue for 75% of the interviewees is the fact that the Product Security Officer has security responsibility throughout the lifetime of the product. When it is in the hands of the customer and a vulnerability is found, it needs to be fixed quickly and customer products updated. This calls for robust update mechanisms and a strong push for security-by- design to minimize the risk of eventual vulnerabilities.

> *The biggest challenge is that when you deliver the product to the customer and later discover a vulnerability, …, although you no longer have control over the product, you are still responsible to maintain its security."*
>
> Security Specialist, European car manufacturer

Standards that are most important by industry

In industrial systems, the most important standard is ISA IEC 62443.

In the automotive industry, key standards are ISO SAE 21434, ISO 24089 based on UN ECE WP29 (in draft) and ISO SAE J3016-2 (in draft).

More than 40% of the interviewees mentioned the NIST guidelines; FIPS and SOC II were also mentioned, as were GDPR and CCPA.

Product Security Programs sought by CPSO

The types of solutions sought, to incorporate security into the product, are tied into product security programs that all are implementing. Product security programs (see a detailed description here) are composed of:

A. Product Security Governance
B. Secure Development Lifecycle
C. Security Measures in Production
D. Product Security Operations

> *It starts with governance, including processes, where we report on critical vulnerabilities. Next, it is R&D processes, to ensure they conform to the secure product development lifecycle. Then there are processes needed for legacy products, active products, end-of-life products…there are documented requirements from design to code reviews to security testing to validation, all the way to disposal of the product in the customer environment.*

A. Product Security Governance

Monitor and Influence Industry Standards

Most of the CPSOs discussed the need to monitor industry standards and, to the extent possible, influence them due to the long lead times required for product development, and the difficulty posed by finding out late in the process that a new standard will be impacting the industry.

> *The company must be ahead of the (regulation) curve. By the time regulations come out, there is only a short time to incorporate them. An example is that the platform architecture will be impacted by the UN ECE regulations that will be adopted this summer, but the team can't wait for that to be adopted and released so is designing and developing in line with what they expect the final regulation to include."*

R&D and Customer Education

Two-thirds of the respondents include product security education as part of their program related to product security governance. Overall, there is a big need for education, both internally and externally. In fact, one company renamed its "Best Practices Standing Committee" to "Education and Training Standing Committee", to emphasize the need to level-up everyone's programs.

B. Secure Development Lifecycle

TARA, Code Verification, Static Code Analysis, Pen Testing

The types of solutions sought, to incorporate security into the product, are tied into the product development organization and are focused on building security into the product from the very beginning of the development cycle. A combination of threat analysis and risk assessment, supply chain analysis, static code analysis, pen testing and other development phase capabilities were mentioned by 100% of the respondents.

Tools that can automate manual tasks that are hard to get right and must be done by virtually everyone in the development team, are key.

> *…pen testing, open source code scanning and analysis are part of our team's effort. It's a partnership because the developers need to understand the flaws and fix them, but they get more skilled over time and security becomes embedded into their daily lives. It's a 'center of excellence' approach".*
>
> Director of Product Security, Fortune 500 industrial automation company

C. Security Measures in Production

Runtime Integrity, Secured Communication, Secure Boot

> *CFI and software hardening are important concepts. Understanding how to do central gateways, firewalls and routing within the product are also important, as is how to implement monitoring.*
>
> Security Systems Engineering and Compliance Manager, Asian car manufacturer

Virtually all the CPSOs interviewed are focused on system integrity and secured communication activities. These include secure boot hardware and software, runtime integrity controls, code obfuscation, and communication encryption. A key consideration for the CPSO is the need for runtime integrity. Because customers are not aware of risks, and because updates happen infrequently (with no guarantee that the customer will be able to implement updates) the need for built-in security is paramount. Runtime integrity was mentioned frequently as an ideal method for ensuring the products are functioning as they should.

> *For tasks that need to be done manually, and by everyone, we need to automate. For example, everyone needs to ensure that buffer overflows don't happen. But if you have 10,000 engineers, even if everyone knows the right thing to do, and tries to do it all the time, we will get it right only 90% of the time. So, a tool to avoid buffer overflows would help. Control flow integrity can do this."*

D. Product Security Operations

Product Updates, Reporting on Security Events

CPSOs overwhelmingly include over-the-air update systems and processes in their programs. It is important to keep field updates as small and infrequent as possible, as users may not have means to update the devices or they prefer to keep them uninterrupted. When updates are conducted, they must be done quickly.

Security monitoring was also mentioned by more than 75% of respondents – this includes software update management, intrusion detection, and more. All respondents stated they include end user or system notification for security events.

Many companies have established a security operations center (SOC) and rely on both behavioral analysis and threat intelligence to ensure that they remain vigilant over their products long after they have shipped to customers. As mentioned above, while updates are important, there is no guarantee that they will be implemented immediately, resulting in even greater pressure for runtime integrity.

While the CPSOs interviewed sometimes used different terminology, all of them mentioned various parts of the full product security program and stressed the importance of the program as a key part of the overall backbone of their role as CPSO.

In summary

CPSO, Product Security Officers, and product security roles, although relatively new, are important and distinct from the role of the Chief Information Security Officer. Product security is highly valued, as shown by its place within the organization. In several of the companies (primarily Fortune 500 companies), product security is a board-level concern, with semi-annual reporting on product security.

The Product Security Officer is an emerging role but one that is easily justified due to the different requirements, span of control and scope. Unlike the CISO, product security must control products long after they are in the customers' hands. As such, product security has fiduciary, SLA and regulatory compliance issues that go far beyond those of IT security. To meet their responsibilities Product Security Officers and CPSOs establish and impose Product Security Programs, from product design through development, production, and post-production phases. Solutions sought address each of the product security program's four phases and are oriented around the security-by-design approach and extended throughout the lifetime of the product.

Product Security Officers play a key role in the organization, but face daunting challenges, as they strive to secure products long after they are in customer hands. During design they face the harsh reality of conflicts between product launch requirements and customer demand. They share many common concerns and are rapidly developing best practices as they respond to customer demands and emerging standards. This report illustrates the importance of building a community of interest where learning and sharing can take place.

To see how Zoom, a high-profile company, suffered without a Product Security Officer and a product security program, and what they did to remedy to the situation, take a look at our recent Product Security series blog post.

Let's continue the conversation in the Product Security Forum on LinkedIn.