CISOs: Why Security Debt is Your Responsibility

& What You Can Do About It Based on New Data

Introduction

As a CISO, security debt in software is your responsibility because it directly impacts the overall security posture of the organization. By addressing security debt, you ensure the protection of sensitive data, safeguard against potential breaches, and maintain the trust of customers and stakeholders.

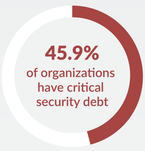
You may be asking yourself, "How risky is security debt? And what's the best way to tackle it?"

Step-by-Step Data Exploration

Here's the data and analysis behind managing security debt, identifying where the most risk is, and navigating it as a CISO.

1 Organizations are drowning in security debt

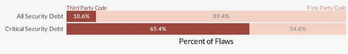
Over 70% of organizations have security debt and nearly half have critical debt (high-severity flaws). Since we define severity as the potential impact on confidentiality, integrity, and availability, these flaws pose a significant risk to organizations.



2 Security debt exists in both first-party and third-party code

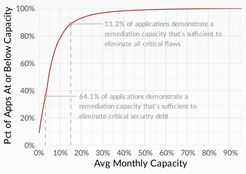
While first-party code makes up the vast majority of overall security debt, most critical security debt comes from third-party code in open-source software. As CISO, it's crucial to consider testing and remediation efforts for both first-party and third-party code continuously throughout development.

Pro tip: make sure scanning tools are part of a single-pane-of-glass platform, so you can easily report progress.



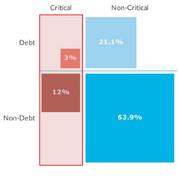
3 Remediation capacity is constrained

Only 64% of applications demonstrate a sustained capacity to eliminate all critical security debt. This means few teams bail fast enough to reverse the tide of debt once it starts rising. As a CISO, it's imperative that policies and guidelines are in place to ensure teams prioritize and promptly address critical security debt first, preventing its accumulation and mitigating potential risks.



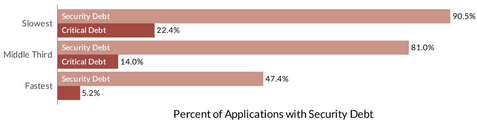
4 Prioritizing which flaws to remediate is essential

Only 15% of all flaws are critical flaws. This subset of flaws represents pound-for-pound the greatest risk exposure to your applications. As CISO, you can help determine the allocation of resources to sustain a program that eliminates critical security debt. Prioritize that 15% and you'll achieve a goal of maximum risk reduction with focused effort.



5 Fixing flaws faster is the path forward

Development teams that fix flaws fastest are 4x less likely to let critical security debt materialize in their applications. As CISO, creating a security culture through developer security education and AI-assisted remediation tools, like Veracode Fix, will help teams fix flaws faster – improving security posture.



Conclusion

Take data-driven action to tackle security debt effectively, including continuous scanning, prioritization, and AI-assisted remediation.

VERACODE

[Download the full report](#) or [get a demo of Veracode Fix today](#)