The link between security maturity and bug bounty success

BY ELEANOR BARLOW · MAY 12, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How your organisation's security maturity level influences the success of a bug bounty program**, including how maturity affects vulnerability discoverability, researcher strategy, and payout expectations.
- **How to realistically assess and improve your security posture**, moving beyond compliance checkboxes to continuous, adversary simulated testing that strengthens resilience and risk management outcomes.
- **How to tailor reconnaissance and bug bounty strategy based on security maturity**, enabling you to prioritize high impact testing, reduce noise, and align resources effectively as your attack surface and risk evolve.

What defines a security maturity posture?

A security maturity posture refers to an organization's ability to detect, manage, and mitigate security vulnerabilities and risks. It reflects how well the organization applies programs, processes, and controls to protect its assets and data. Generally, a higher security maturity posture indicates a stronger capability to identify and respond to cyber threats.

'Organizations with mature cybersecurity practices experience a 67% decrease in the average cost of a data breach.'- GoStack

What does this have to do with bug bounty programs?

Establishing a bug bounty program is not the first step in becoming mature. It's a hallmark of a company that has reached a certain level of security maturity. The adoption of bug bounty programs signals that the organization has already laid a solid foundation of internal security practices, risk management protocols, and incident response capabilities. By asking external researchers to test their systems, the company demonstrates confidence in its security posture and a proactive commitment to continuous improvement.

Challenges often emerge when organizations equate their security maturity with the presence of formal processes or adherence to compliance frameworks. While regulatory alignment and increased security investment are important factors to drive security maturity, they do not guarantee a resilient security posture, especially in large, complex enterprises with expansive attack surfaces. It's a common

misconception that a bigger budget automatically translates into better security. In reality, true maturity comes from how effectively that investment is operationalized across the organization.

> "*While individual business units or teams may demonstrate compliance or conduct isolated penetration tests, the lack of coordinated, end-to-end security validation may leave critical exposure points unchecked. Advanced adversaries exploit these entry points, particularly where independently hardened systems integrations may not have been tested effectively. Malicious threat actors do not care about in-scope, out-of-scope, or testing windows but are driven by achieving their goals. To move beyond surface-level compliance and effectively reduce cyber risk, organizations must adopt continuous, adversary-simulated testing that spans their entire attack surface and mimics real-world threat behaviors.*"
>
> **Harry Grobbelaar, Chief Revenue Officer, Intigriti**

The 2024 SnowFlake example explored

A leading cloud data platform provider, known as SnowFlake, was the target of one of the most significant data breaches to date. In December of 2024, the company was besieged by a Scatter Spider attack where SnowFlake's data was compromised, but so was the data of their customers. This included Personable Identifiable Information (PII) data from AT&T, Ticketmaster, Neiman Marcus, Santander Bank, and more. Once collected, the data was leaked and sold on the dark web.

A month before the attack, the company had 10,618 customers, including more than 800 members of the Forbes Global 2000. This example shows that no matter the company size, and even with security frameworks in place, all businesses are susceptible to a cyber attack. This is why it's important to be realistic about the level of security maturity, to test it, and adapt your strategy to move with the growing threat landscape.

How security maturity posture influences bug discovery and payout

Depending on the environment presented, bug bounty hunters will tailor their strategy and expectations, and the security maturity level will impact the volume of easily discoverable bugs, scope, and cost of payouts.

In organizations with low security posture maturity, a higher volume of discoverable bugs and a broader scope of bug types are expected. If the security maturity is low, low-hanging fruit is often easily accessible. This means weaknesses and vulnerabilities within systems that threat actors can easily and quickly exploit at little cost to themselves will be targeted. Bug bounty teams can broaden their search for low-hanging misconfigurations first and then work their way up to more complicated vulnerabilities.

Regarding payout, low-maturity organizations will often have budget limitations, which can impact the scope. A lack of people and experience with IT teams may also impact the ability and speed to act on vulnerabilities once they have been identified by bug bounty teams. But the important thing here is visibility, so that companies with smaller budgets and resources can prioritize patches and organize remediation efforts based on impact.

Findings for high-security maturity organizations require creativity and effort, and usually a higher payout for complex new findings. High-security maturity organizations tend to have a higher budget,

which means severity-based or impact-based payments, and high-severity findings for a greater reward. In addition, updates are usually more frequent, and remediation timeframes are clear-cut.

'Organizations with a high level of cyber maturity experience significantly lower costs associated with data breaches, ransomware attacks, and other cyber incidents.'- Vohkus

High-security maturity orgs will likely have fewer bugs, as security testing and automation should be in place to sweep up the low-hanging vulnerabilities.

'Organizations utilizing automated monitoring tools can detect 66% more threats, enhancing their ability to respond proactively'- moldstud

Recon strategy based on security maturity level

Regardless of security posture level, build or adjust your recon strategy to make your bug bounty more effective, reduce noise, and increase ROSI.

- Low security maturity organizations should widen their analysis to look at all types of vulnerabilities.
- High security maturity organizations should go granular with their analysis and scope out areas of interest together.
- Re-analyze security maturity regularly. Especially after organizational changes, new system integration, and company expansion.

'Implementing a Cybersecurity Maturity Model can lead to a 25% reduction in cybersecurity costs by streamlining operations and reducing waste.'- CIOinsights

Don't know your level of security maturity?

For organizations that are unsure of their maturity level, start by ensuring compliance with cybersecurity frameworks such as NIST and ISO. As well as GDPR, HIPAA, and PCI-DSS if they apply to your industry. There are multiple requirements specific to every industry and region, so ensure that the necessary steps have been taken to meet the required standards for your company.

Vulnerability Disclosure Programs (VDPs) can help organizations boost business credibility and resilience, as well as simplify compliance processes. The primary function of a VDP is to provide a structured, transparent, and efficient process for the identification, communication, and remediation of security vulnerabilities.

Penetration testing is also a great way to gain visibility on your security maturity. Look for one that supports time-boxed assessments aligned with a client-defined methodology, so that it can be tailored to specific testing requirements.

Next steps and recommendations

1. Make no assumptions. Adapt your approach, review security tools and applications, and be realistic about your company's security maturity posture to improve it and adapt to the growing threat landscape.

2. Integrate continuous, real-world testing into your defense strategy with a bug bounty program. By inviting skilled ethical hackers to identify vulnerabilities that may go undetected by traditional methods, these programs foster a culture of continuous improvement and adaptive risk management. Refine security policies, improve incident response, and prioritize remediation efforts.

3. Remember, security success isn't about cost or volume, but impact, on both sides. Direct efforts from the ground up to instill a culture of proactive security testing to optimize resources.

To learn more about how Intigriti's bug bounty program can enhance your security maturity posture, contact the team today.

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.