Justifying cybersecurity budgets: The power of cyber threat analysis

BY ANNA HAMMOND · OCTOBER 2, 2024 · LAST UPDATED ON MARCH 6, 2025

Cybersecurity is not just an IT concern, but a business imperative. Cyber threats pose significant financial, reputational, and legal risks. From data breaches that lay bare sensitive information to ransomware attacks that paralyze operations, the costs of insufficient cybersecurity can be catastrophic.

Yet, many security teams struggle to justify the budget needed to bolster their defenses. This is where cyber threat analysis comes into play—a powerful tool that can transform technical findings into a compelling business case. In this guide, you'll learn how to use the process to get buy-in and approval for cybersecurity budget. From performing the evaluation to putting your findings into a compelling case that'll resonate with budget-holders, we've got you covered.

Cyber threat analysis: an overview

The primary purpose of cyber threat analysis is to:

- Evaluate the nature and scope of cyber threats
- Determine their potential impact
- Develop strategies to safeguard against them.

The benefits of cyber threat analysis are manifold. It enhances the organization's security posture, improves incident response capabilities, and provides a better understanding of the organization's risk profile. Additionally, it helps ensure compliance with regulatory requirements.

However, the process is not without challenges, such as the rapidly evolving threat landscape and the need to balance security with operational needs. That begs the question, is it worth doing? Absolutely.

Cyber threat analysis is a vital component of an organization's overall cybersecurity strategy. It helps protect sensitive data, maintain operational continuity, and safeguard against financial and reputational damage. In other words, cyber threat analysis is not only worth doing but should be considered a priority.

What types of threats are found during a cyber threat analysis?

During analysis, several types of threats are typically identified and evaluated. These can originate from various sources and exploit different vulnerabilities. Here is a list of common threats found:

- **Malware:** Malicious software programs that can disrupt operations, steal data, or demand payment to restore access to systems.

- **Phishing:** Tricking individuals into divulging sensitive information or performing actions that compromise security.
- **Spear-phishing and whaling:** Targeted forms of phishing that focus on specific individuals or high-profile targets.
- **Denial of Service (DoS):** Overwhelms systems with excessive traffic, making them unavailable to users.
- **Data breaches:** Unauthorized access to sensitive information, leading to data exfiltration and theft.
- **Advanced Persistent Threats (APTs):** Sophisticated, long-term attacks targeting specific organizations or industries.
- **Man-in-the-Middle (MitM) attacks:** Intercepts communications between two parties.
- **Zero-day exploits:** Takes advantage of unknown vulnerabilities in software.
- **Insider threats:** Comes from malicious actions by employees or contractors, as well as accidental data leaks due to human error.
- **Supply chain attacks:** Compromises third-party vendors or suppliers to gain access to the target organization.

We've highlighted some common threats here, but remember, the digital landscape is constantly evolving, with new vulnerabilities emerging regularly.

A step-by-step guide to conducting cyber threat analysis

This process will help you identify, assess, and mitigate potential cyber threats to your organization. As a result, you'll be better equipped to protect your critical assets and respond effectively to security incidents.

Step 1: Define the scope

The first step is to define the goals and scope of the analysis. This includes identifying the specific objectives, such as protecting sensitive data or securing critical infrastructure, and determining the scope, such as whether it will cover the entire organization or specific departments.

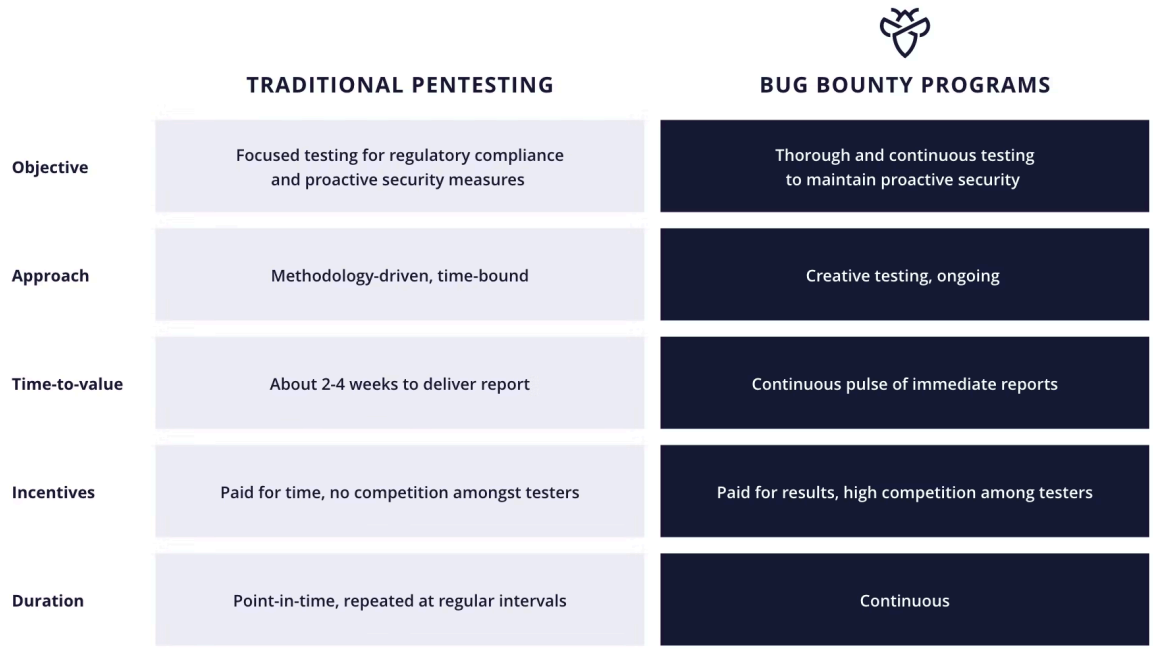
Step 2: Gather information

The next step is to pinpoint and rank critical organizational assets. This includes identifying valuable assets such as customer data, intellectual property, and critical systems. By ranking these assets based on their importance and potential impact if compromised, organizations can prioritize their protection efforts. This step is crucial for ensuring that the most critical assets receive the highest level of security.

Step 3: Identify potential threats

The next step is to conduct a risk assessment, scrutinizing the potential vulnerabilities and weaknesses within an organization's systems and infrastructure. Cyber threat analysis tools, including vulnerability scanners and threat intelligence platforms, are employed to detect and understand these vulnerabilities.

Penetration testing (pentesting) is another solution to provide intelligence. They work by simulating cyber-attacks during a time-boxed period to identify and fix security gaps following a set methodology. An alternative or complementary solution would be a bug bounty program—which is like pentesting, but with some differences. Primarily, the scope of a bug bounty program is wider than a pentest, and the testing approach is creative and ongoing.



	TRADITIONAL PENTESTING	BUG BOUNTY PROGRAMS
Objective	Focused testing for regulatory compliance and proactive security measures	Thorough and continuous testing to maintain proactive security
Approach	Methodology-driven, time-bound	Creative testing, ongoing
Time-to-value	About 2-4 weeks to deliver report	Continuous pulse of immediate reports
Incentives	Paid for time, no competition amongst testers	Paid for results, high competition among testers
Duration	Point-in-time, repeated at regular intervals	Continuous

This process is instrumental in pinpointing the areas where an organization is most susceptible to cyber threats.

Step 4: Prioritize threats

Assessing the likelihood and potential impact of identified vulnerabilities is a critical aspect of cyber threat analysis. By examining historical data, industry patterns, and threat intelligence reports, organizations can ascertain the probability of various cyber threats and the potential repercussions of their occurrence.

This evaluation is instrumental in prioritizing mitigation strategies and resource allocation. For instance, a threat deemed highly probable with significant impact warrants immediate attention.

Step 5: Develop mitigation strategies

The next phase is the development of a plan to address the identified risks. This plan should include specific actions, such as implementing security controls, training employees, and investing in advanced security technologies. The plan should be tailored to the organization's unique needs and risk tolerance.

Step 6: Using your findings to justify budget

To construct a compelling cybersecurity budget proposal, it is essential to ensure that it is in harmony with the organization's strategic objectives. Utilize data-driven insights from cyber security threat analysis to underpin your recommendations. Demonstrate how augmented budgets for cybersecurity can translate to enhanced risk management and operational resilience.

Return on Security Investment (ROSI) can provide a powerful gauge of your cybersecurity spending's impact. It quantifies the financial value of security measures by weighing the risk and cost reductions they bring. By comparing security implementation costs with prevented financial losses, ROSI helps organizations pinpoint the effectiveness of their security expenditure. This metric empowers strategic decisions, spotlighting the economic advantages of investing in robust security systems to preserve operational continuity and safeguard your organization's reputation.

Step 7: Implement, review and improve

Establish a feedback loop to continuously improve your threat analysis process. Document lessons learned from incidents and use them to refine your threat analysis approach.

How Intigriti's platform can help

By investing in robust cyber threat analysis capabilities, organizations can transform technical findings into actionable business insights, reinforcing the case for increased cybersecurity budgets and ensuring long-term resilience against cyber threats.

Intigriti's bug bounty platform offers clients valuable historical data and a real-time overview of the most commonly found vulnerabilities in their systems. This knowledge provides tangible evidence of areas that require focus, helping to allocate cybersecurity budget effectively and demonstrating the value of an ongoing bug bounty program.

To discover more about what security teams can achieve by launching a bug bounty program with Intigriti, get in touch today.