
CYBERSECURITY INSIGHTS

# Sharpening SLAs for Vulnerability Management

Building secure business partnerships

EBOOK

# Table of contents

# A note from Stijn, Intigriti's CEO and Founder

**At Intigriti, we recognize the relentless pressure business leaders face to not only survive but also prosper. For cybersecurity leaders, the challenge is even greater. They must constantly guard against a rapidly changing threat landscape with limited resources while meeting high expectations from stakeholders.**

Fortunately, cybersecurity budgets are on the rise, with Gartner predicting a 14.3% increase in global security and risk management spending. This boost reflects the need to address the expanding attack surface while simultaneously complying with new and emerging regulatory standards.

Another silver lining of robust cybersecurity practices is the competitive advantage it provides. When businesses evaluate a new service provider, the decision hinges on more than just features; it centers on security and reliability too. Cybersecurity service-level agreements (SLAs) are crucial in this context, offering clear, actionable standards for performance and accountability.

Our report, "Sharpening SLAs in Vulnerability Management," reveals the current benchmarks for identifying and handling data breaches. Refining and setting standards for this process is essential not only for customer interactions but also for directing the priorities and focus of security teams. Detecting vulnerabilities, however, is just one aspect. Promptly addressing and communicating these issues is equally critical to maintaining your organization's security.

By equipping security teams with definitive guidelines and the necessary tools to counter threats, we establish a strong and resilient cybersecurity framework that benefits employees, customers, and the industry at large.

Now, more than ever, it is crucial for leaders to step up and invest in these areas. Let us lead the change in fortifying our defenses, setting new standards in cybersecurity, and ensuring a safer digital future for all. Together, we can transform challenges into opportunities for growth and innovation.

**Stijn Jans**
**CEO AND FOUNDER**

[1] go.intigriti.com/gartner-prediction

# About Intigriti

**Intigriti is the trusted leader in crowdsourced security. Since 2016, we've empowered the world's largest organizations to proactively identify and address vulnerabilities before they're exploited by cybercriminals. Harnessing the skills and expertise of our 100,000+ researchers, businesses can detect vulnerabilities as soon as they surface, avoiding costly damages from security breaches.**

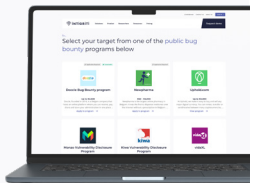
Through our meticulous triaging process, commitment to legal compliance, and unparalleled customer service, we deliver the utmost reliability and assurance for our customers. Intigriti is proud to be the bug bounty platform of choice for industry leaders such as Coca-Cola, Microsoft, and Intel, safeguarding their digital assets in an ever-evolving threat landscape.

## Intigriti's services

- Bug bounty programs
- Vulnerability disclosure programs (VDPs)
- Pentesting-as-a-Service (PTaaS)
- Live hacking events

**400+**

active bug bounty programs



**100K+**

security researchers

**9.2**

Net Promoter Score

**1.4 days**

validation period for vulnerability reports*

*12 business hours is the time it takes on average for Intigriti to review and validate a vulnerability report

# Methodology

**This report combines qualitative and quantitative research into how organizations manage vulnerabilities and use service-level agreements for this purpose.**

The survey was conducted in May 2024 by an external agency. It includes 250 responses from information security (InfoSec) professionals in the UK and the US. Data was rounded for clarity. Respondents came from across 12 industries and held the following InfoSec job titles:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Technology Officer (CTO)
- Chief Operations Officer
- Global Security Manager
- VP of Technology
- Security Analyst
- Security Operations Manager
- Security Engineer
- Head of Security Architecture
- Security Platform Lead
- Global IT Security Operational Risk Lead
- Senior Specialist Information Security (Application Security)
- Application Security Manager

# The true cost of a breach

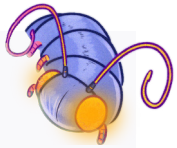
**The majority of survey participants estimate the financial impact of a data breach to be up to £500,000 pounds (or US$600,000). Yet, research from IBM[2] 2024 revealed that, globally, the average cost of a data breach soared to an all-time high of US$4.88 million—a 10% increase over last year and the highest total ever. While the specific financial impacts of a breach can vary between organizations, it is evident that the consequences are substantial and could be potentially irreversible.**

One effective strategy to reduce these risks involves collaborating with ethical hackers. Also known as security researchers, these professionals identify and report vulnerabilities to the relevant organizations in good faith, helping to prevent potential breaches.

### Discover more about ethical hackers

Scan the QR-code or visit go.intigriti.com/ethical-hacker-insights-report-2024-sla


[2]go.intigriti.com/ibm-research

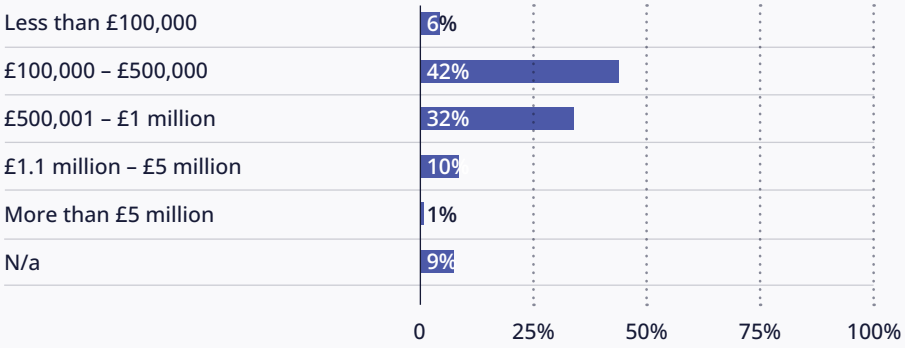


**Estimated financial cost for organizations if a critical vulnerability leads to a data breach:**

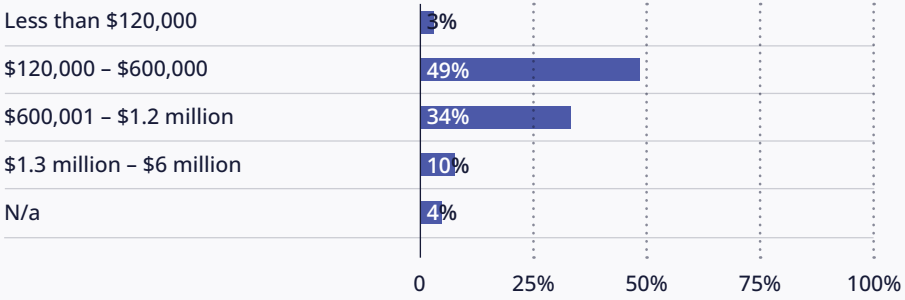
**Direct cost examples:** Fines, legal fees, breach notification

**Indirect cost examples:** Reputation damage, customer churn

**United Kingdom**




**United States**



# What are SLAs and how do they apply to vulnerability management?

**A Service Level Agreement (SLA) is a formal document outlining the expected level of service from a provider to a customer. SLAs are essential for establishing clear expectations and accountability, detailing specifics such as scope of work, quality, responsibilities, and timelines.**

In the context of cybersecurity, SLAs are particularly crucial as they ensure that services adhere to agreed-upon security standards and performance metrics. Specifically, in vulnerability management, SLAs define the processes for how security flaws in a service provider's IT infrastructure are identified, addressed, and resolved by the business.

Failing to adhere to an SLA can lead to significant consequences for business efficiency and profitability. Potential repercussions include financial penalties, damage to reputation, customer loss, legal challenges, operational disruptions, strained relationships, and increased costs. Therefore, crafting comprehensive and clear SLAs is fundamental to maintaining trust and ensuring mutual success in any business relationship.


RESEARCHER
**tamaytandiran**

# SLA stages for vulnerability management

## Key components of an SLA in this field typically include:

**01 Initial acknowledgment**

This section defines how quickly a reported vulnerability will be responded to. It also sets expectations for the time it will take them to begin remediation after a vulnerability is identified. During this stage, a severity score is applied.

**02 Mitigation**

Here, the timeframe within which a vulnerability must be fully resolved or mitigated after it's been acknowledged is defined.

**03 Disclosure**

SLAs should detail how the service provider will collaborate with the discoverer of the vulnerability for a coordinated disclosure, informing stakeholders and regulatory bodies about the incident and corrective actions.

**04 Performance metrics**

These are benchmarks for assessing the effectiveness of the vulnerability management process. Metrics might include the number of vulnerabilities detected, the percentage successfully mitigated, and the time taken to mitigate vulnerabilities against the SLA standards.

# Industry benchmarks for vulnerability management

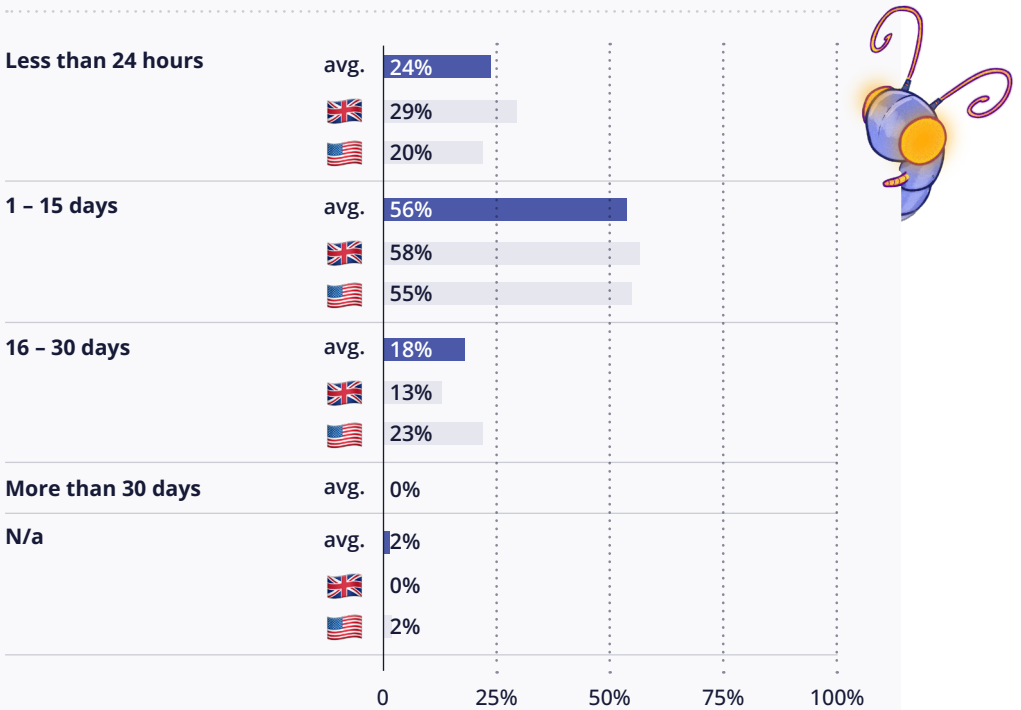
## 1. Initial acknowledgement

**Swift acknowledgement instills confidence that concerns are being taken seriously and actioned. In many cases, vulnerabilities are reported to organizations by external security researchers. If a researcher doesn't receive a response to their report, they might think it didn't reach the business successfully or—even worse—that the business is actively ignoring the vulnerability.**

For a critical to exceptional vulnerability, any longer than 24 hours is too slow for an initial response. Yet, three–quarters (75%) of businesses are missing this window. More urgency is needed—an unpatched exceptional vulnerability that was known about but not acted upon could result in potential breaches, undesirable headlines, customer complaints, loss of business, and more.

Additionally, ethical hackers may publicly disclose vulnerabilities when vendors ignore their reports or fail to fix issues within a reasonable timeframe. This approach pressures vendors to act and informs users about potential risks, promoting quicker resolution and enhancing user safety through awareness.

**What are your company's SLAs in terms of Initial acknowledgement for a critical to exceptional vulnerability?**



## 1.1 Severity scoring

**Most organizations are following a blend of internal ratings (70%) with the Common Vulnerability Scoring System (CVSS)[3] (34%) and OWASP Risk Rating[4] (29%) to determine the severity of reported vulnerabilities and prioritize response efforts. Critical issues may require immediate action, while less severe issues can be addressed through routine updates.**

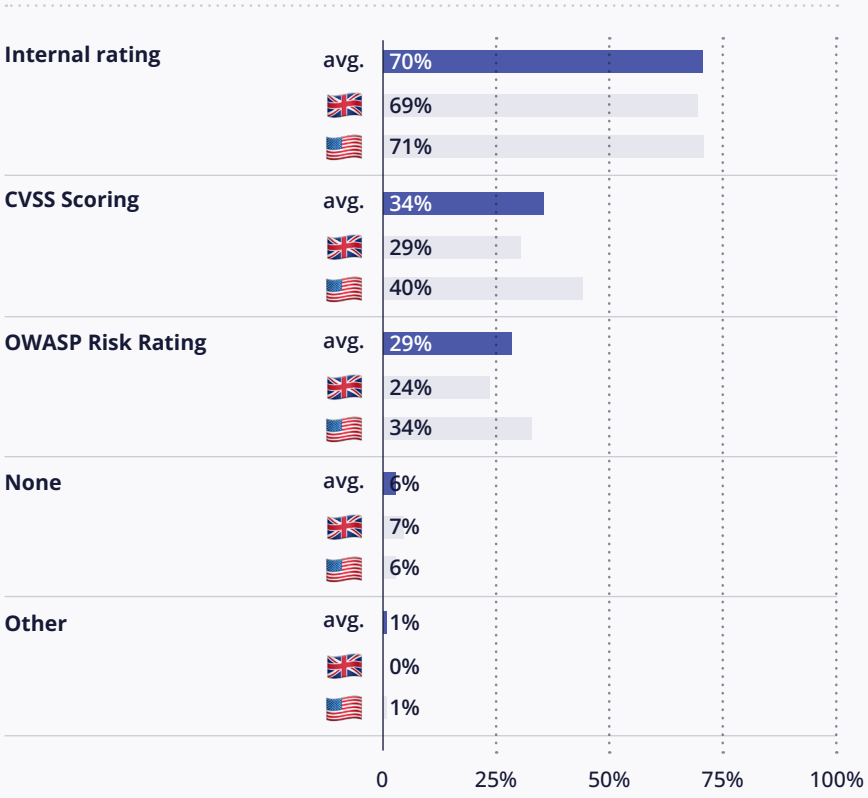
In an ideal world, 100% of organizations would be combining their own system with an industrialized standard. Since every company has different risk and threat models, the final severity of a vulnerability can only be determined after thorough examination by their own security analysts.

> Prioritizing issues incorrectly can have significant implications. We've seen incidences where a submission comes in and it's not classified as something the company wants to fix urgently—then it becomes more serious than originally thought. That's why benchmarking with outside information is so important.

**Inti De Ceukelaire**
CHIEF HACKER OFFICER

İNTİGRİTİ

**Which systems are used to score the severity of vulnerabilities once discovered?**




**NB:** Respondents could pick more than one option

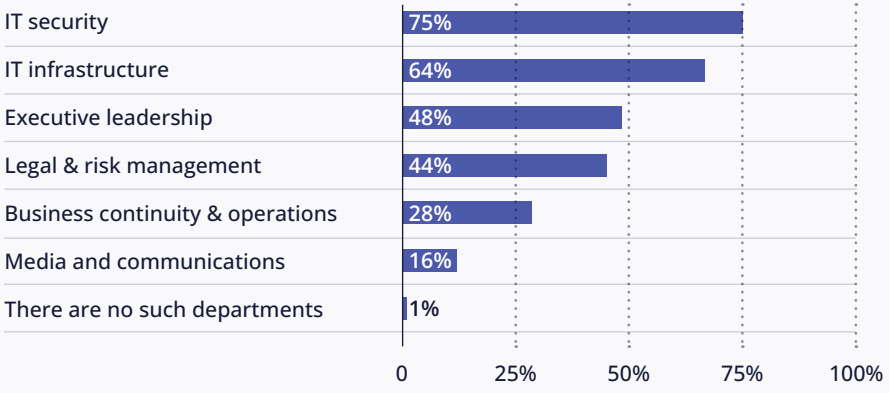
[3]go.intigriti.com/cvss-calculator
[4]go.intigriti.com/owasp

## 1.2 Stakeholder engagement for scoring critical vulnerabilities

**More than half (52%) of companies do not consult their executive leadership team when a critical vulnerability arises, and only 44% involve legal and risk management in the assessment process. Considering that certain industries must legally report unauthorized access within a specific timeframe, involving these departments is essential to prevent severe penalties.**

It is also notable that over one-third (36%) of respondents do not consult their IT infrastructure teams, which typically include professionals like network engineers, system administrators, and application developers. Since vulnerabilities often originate from human errors in product development and digital asset management, involving these professionals early is key. Their input can accelerate the analysis of the likely severity of a vulnerability and help in quicker mitigation of potential breaches.

**Which departments are typically consulted in your organization to assess the severity and impact of a critical vulnerability?**



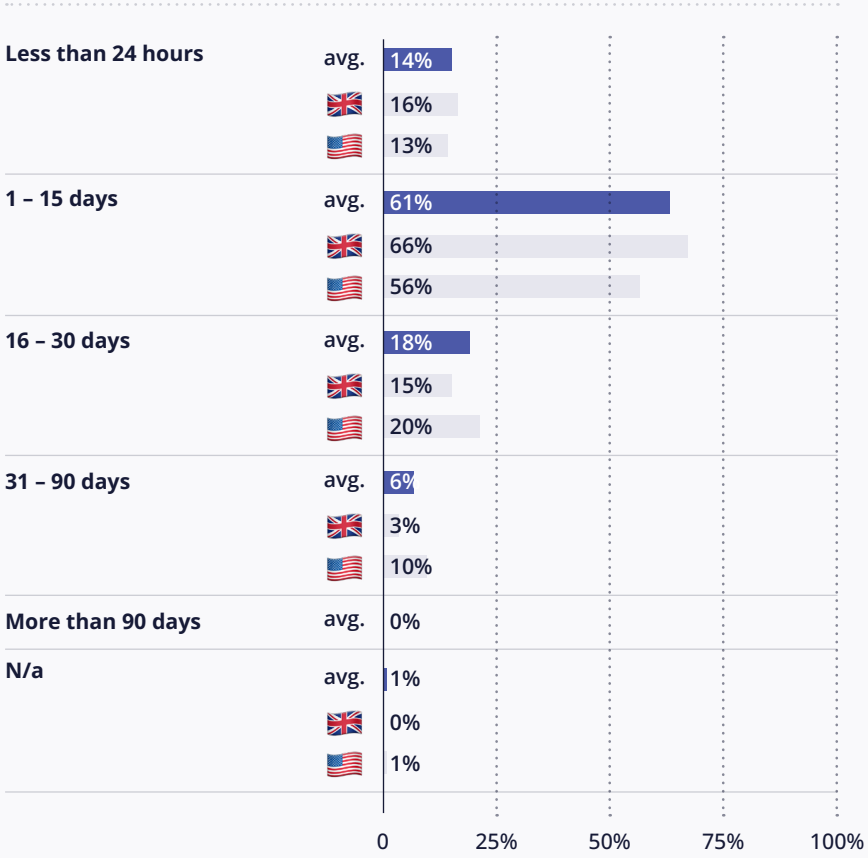

**NB:** Respondents could pick more than one option

## 2. Mitigation

**During the mitigation phase, cybersecurity teams collaborate to quickly address threats and begin resolving vulnerabilities. This process includes implementing strategies based on severity and potential impact, like applying patches, isolating compromised systems, or setting up temporary controls to neutralize the threat.**

Urgent remediation is essential to limit damage, prevent data breaches, reduce the risk of further attacks, and preserve system integrity. For critical vulnerabilities, immediate action is imperative. Based on survey results, 61% of businesses aim to resolve a critical to exceptional vulnerability within 15 days (about 2 weeks), with the UK (66%) striving for faster mitigation than the US (56%).

**What are your company's SLAs in terms of a mitigation plan for a critical to exceptional vulnerability?**

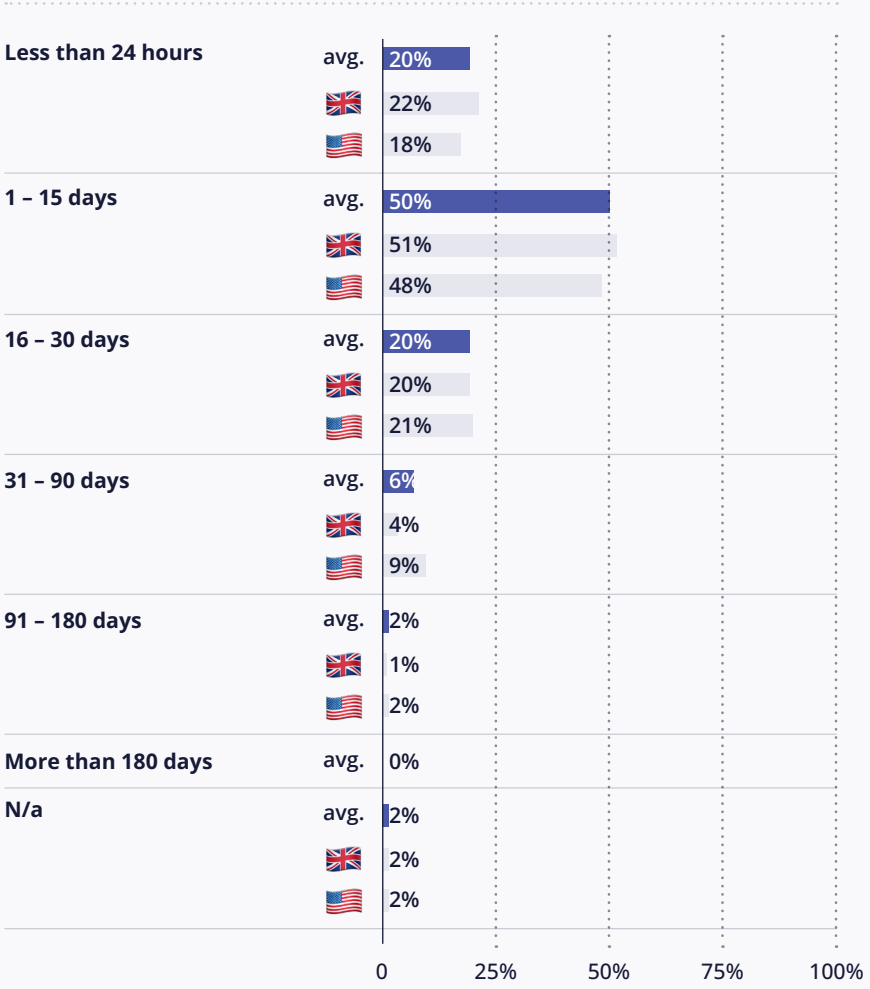


# 3. Disclosure

**This stage of vulnerability management involves collaboration between the discoverer of the vulnerability and the service provider to ensure a coordinated release of information post-mitigation. Organizations should inform all relevant stakeholders, affected parties, and data breach regulators about the incident. Communication should also include the measures taken to address the vulnerability.**

While it's reassuring that one–fifth of respondents globally disclose critical vulnerabilities in less than 24 hours, it's surprising that more than a quarter (28%) take over 16 days. In the UK, 25% of respondents who take this long risk breaking the law. Under Article 33 of the General Data Protection Regulation (GDPR), organizations are required to report breaches within 72 hours of discovery[5] without undue delay (if it meets the threshold for reporting).

**What are your company's SLAs in terms of disclosure for a critical to exceptional vulnerability?**




[5]go.intigriti.com/article-33

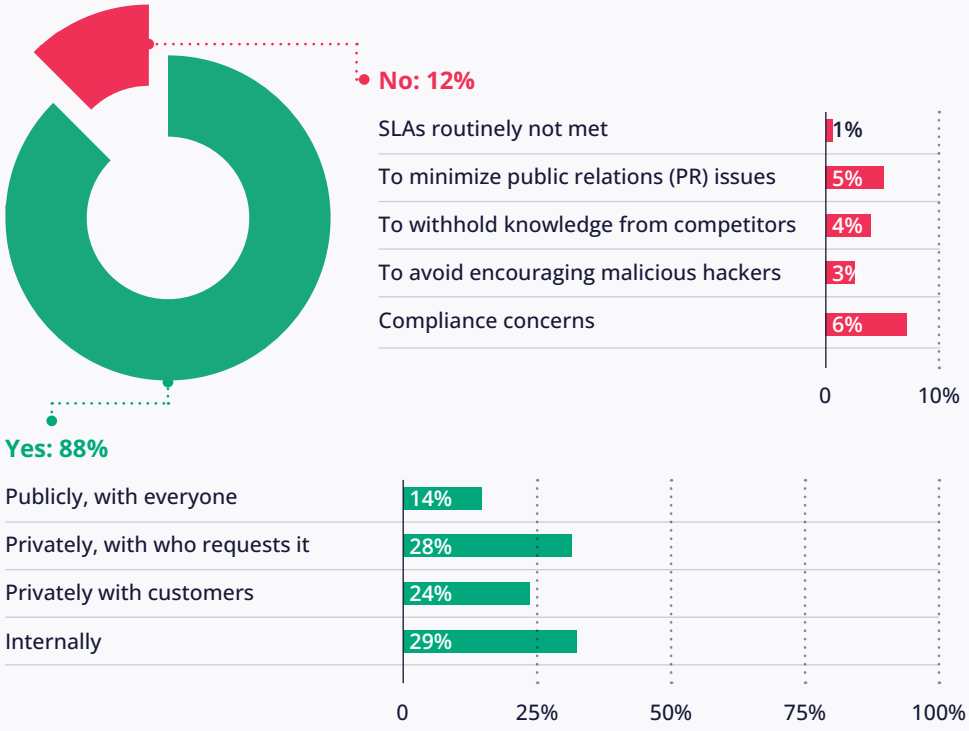
# Driving security transparency and building trust with clients through SLAs

**Of our respondents, 88% share their service-level agreements publicly or privately. It's encouraging to see that two-thirds (66%) of these respondents share their SLAs with external stakeholders.**

Incorporating vulnerability management into your cybersecurity SLA not only prepares your organization for vulnerability reports but can also be a decisive factor in securing new business.

When selecting service providers, SLAs and adherence to security standards are typically assessed by security and legal teams—both of whom will have real concern over the speed at which vulnerabilities are acknowledged, mitigated and disclosed. Having a strong process in place, therefore, can be the difference between winning and losing new business.

**Do you privately or publicly share SLAs? If not, why not?**



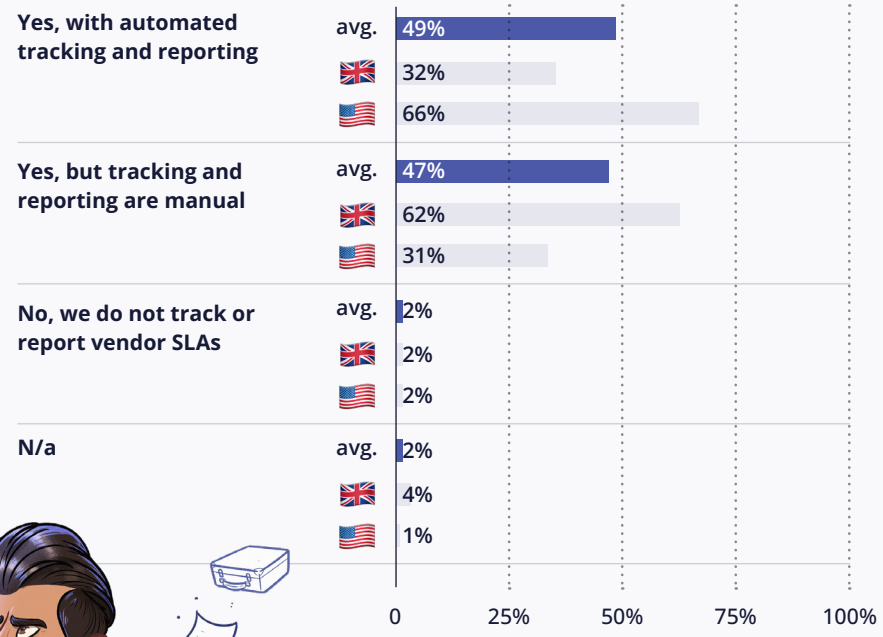

**NB:** Respondents could pick more than one option

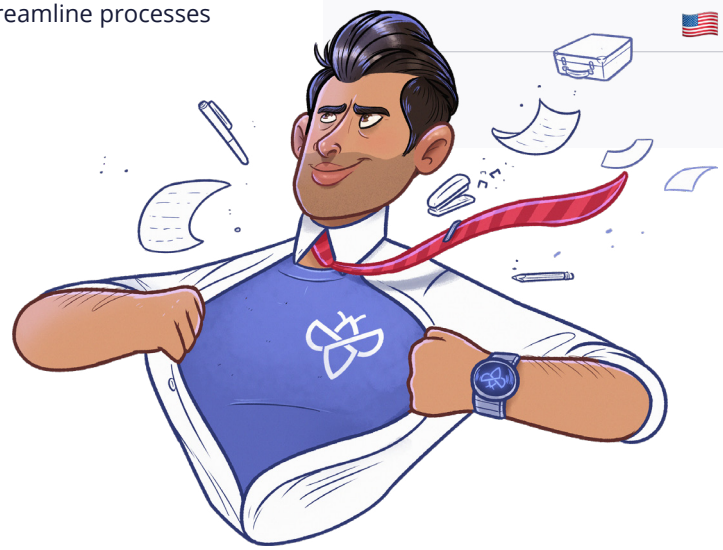
# Strengthening supply chain security with SLAs

**A significant 96% of survey participants have established systems to monitor and report on compliance with vulnerability disclosure SLAs for their contracted vendors. This proactive approach significantly enhances the ability to identify and address security vulnerabilities swiftly throughout the supply chain.**

However, nearly half (47%) of the respondents admit that their tracking and reporting process is manual, which increases the risk of human error and potentially delays the detection and mitigation of security threats. In a comparative analysis between regions, the US outperforms the UK in the adoption of automated systems for this purpose. Specifically, two-thirds (66%) of US respondents utilize automated tools for tracking and reporting on vulnerability disclosures, in stark contrast to only 32% of their UK counterparts. This disparity highlights a significant difference in the adoption of technology solutions that can streamline processes and reduce errors in critical security management tasks.

**Does your organization track and report on compliance with vulnerability disclosure SLAs for vendors under contractual agreements?**



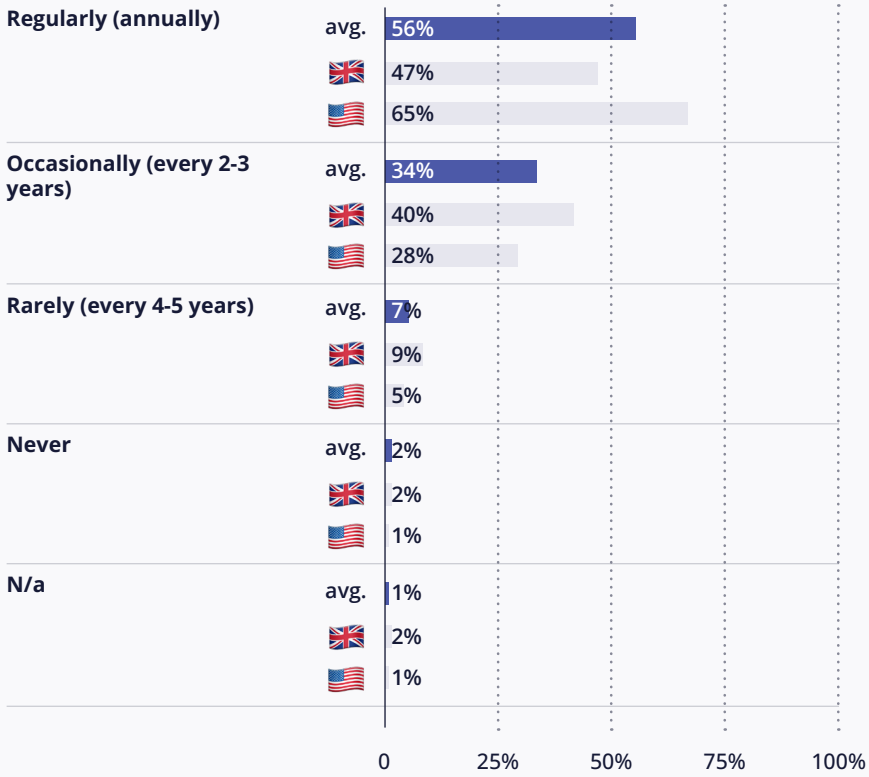



# Assessing the financial impact of mitigating critical vulnerabilities vs data breach expenses

**At the other end of the spectrum, nearly half (43%) of organizations don't conduct regular cost-benefit analyses to weigh up vulnerability remediation expenses against the costs of a data breach. However, the US are better at prioritizing this task, with almost two-thirds (65%) performing regular tests compared to under half (47%) of UK respondents.**

Without this cost-benefit analysis, ensuring safety becomes challenging, and justifying cybersecurity expenditures is more difficult, potentially resulting in insufficient buy-in and investment. US organizations often surpass UK organizations in adopting proactive security testing measures, such as bug bounty programs, to identify vulnerabilities before malicious hackers can exploit them. The higher prevalence of regular cost-benefit analyses is likely a significant factor contributing to this advantage.

**How frequently, if at all, does your organization conduct cost-benefit analyses to evaluate the expenses associated with resolving critical vulnerabilities compared to the potential costs of a data breach?**



# Post-incident reviews and beyond

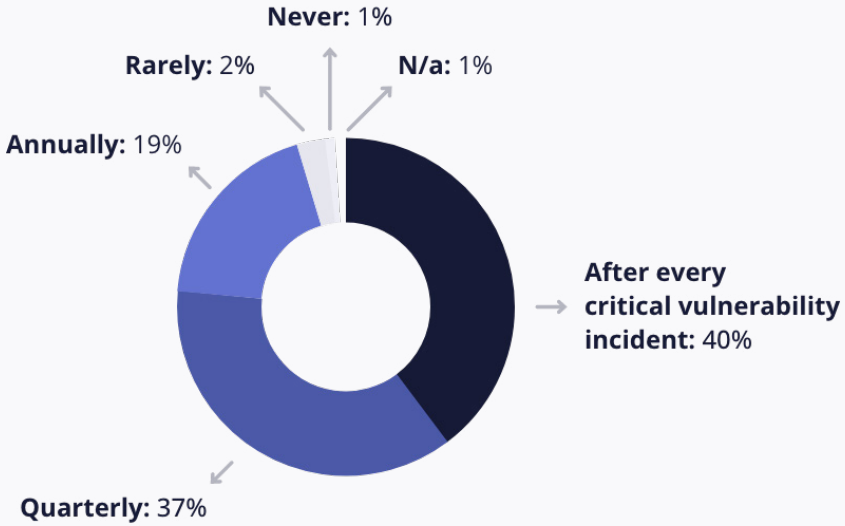
Organizations should not underestimate the value of post-incident reviews, which offer an opportunity to reunite teams to analyze the details of an incident and prevent its recurrence. Frequently, the insights gained from these reviews can furnish the evidence needed by security teams to secure additional cybersecurity funding and drive change within the company.

> Post-incident reviews are essential to maximizing the value of vulnerability resolution, as you get to take a step back and identify possible issues in other parts of the business, beyond engineering. For example, process flaws, commercial expectations, legal and risk posture, and the actual cost of functionality. Then you've got all the information you need to make a business case to maintain and improve security operations.

**Koen Heyns**
COO

INTIGRITI

**How often does your organization conduct post-incident reviews following the resolution of critical vulnerabilities to assess the effectiveness of the response and SLAs?**



# 6 ways to sharpen vulnerability management with Intigriti

**A robust service-level agreement can significantly enhance security, boost client acquisition, and increase an organization's trustworthiness, meaning there's a lot to gain. However, there's also a lot to lose—failing to fulfill these promises can lead to penalties, incomplete payments, or the necessity to issue refunds.**

Fortunately, platforms like Intigriti streamline the processes for security teams, allowing them to address vulnerability reports with greater efficiency and speed, from initial acknowledgment to disclosure.

## 1. Triaging vulnerabilities enables security teams to respond faster

By launching a bug bounty program or vulnerability disclosure program on Intigriti's platform, organizations provide an easier means by which ethical hackers can report vulnerabilities. By default, all vulnerability submissions enter a triage process. The average response time is 12 hours for Intigriti's security analysts to review and validate a report. With this initial screening process, internal security teams already know the vulnerability report is:

- Unique
- Reproducible
- Genuine and in-scope
- Written well with adequate information provided
- Assessed for severity

Having this process taken care of removes the pressure from internal security teams and cancels out the noise of invalid submissions, saving time and allowing them to focus on relevant vulnerabilities that genuinely require their attention.

## 2. Standardizing severity scoring

Standardizing severity scoring for vulnerability reports enhances consistency, prioritization, and communication, ensuring critical issues are addressed first. It also aids in resource allocation, compliance, and benchmarking, ultimately improving an organization's security posture and reducing the risk of breaches.

The following formula serves as a guideline when suggesting a report's severity on Intigriti's platform:

**CVSS = CVSSv3 base score + business impact modifier (optional)**

Intigriti uses the CVSS v3 industry standard[6] as a baseline for severity scoring. There can always be escalating or mitigating factors given the provided context, but the baseline helps provide a faster and more accurate reading for security teams to work from.

## 3. Collaboration with the vulnerability discoverer speeds up mitigation

Security researchers often become invaluable assets to companies because they allow organizations to gain additional insights. For example, researchers can detail their discovery process of a vulnerability, helping security teams to assess the severity faster and decide on the most appropriate actions.

## 4. Maintaining control over communications

A timely initial acknowledgement helps remove the risk of a vulnerability being disclosed without authority and encourages a more coordinated approach.

Intigriti's platform takes this a step further by ensuring these conditions are legally binding. The community sign-up process requires ethical hackers to read and accept the researcher T&Cs[7], which include strict guidelines on confidentiality, non-disclosure of vulnerabilities, data-processing, and more. Plus, Intigriti acts as the middleperson in terms of mediation and communication.

[6] go.intigriti.com/cvssv3
[7] go.intigriti.com/researcher-terms-conditions

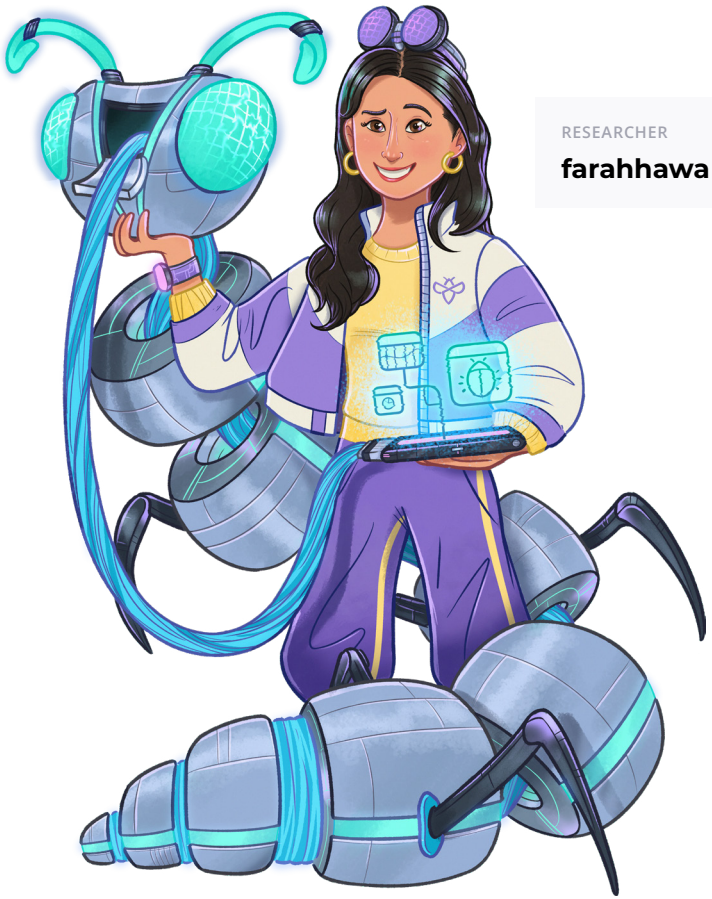
## 5. Proving performance metrics

Intigriti's platform tracks and displays the average response time for each bug bounty program. Having this available is beneficial for organizations wanting to quantify and prove their rapid initial acknowledgement rate.

## 6. Complying with regulations and security standards

Numerous regulatory frameworks require robust security and data safeguarding practices. A Vulnerability Disclosure Program (VDP) assists in meeting requirements from standards like GDPR, HIPAA, and PCI DSS.

> By establishing explicit rules and legal safeguards for those reporting vulnerabilities, a VDP reduces the likelihood of legal conflicts and fosters greater cooperation with the security community.



# Disclosure diary: the journey to effective response

Organizations can effectively prepare for critical vulnerability disclosures by establishing a clear response strategy. Here is what an effective response might entail when working with a bug bounty platform, like Intigriti:

**Week 1**

### **Day 1** • Thursday

- Ethical hacker identifies and documents a critical vulnerability
- Ethical hacker notifies the organization, providing initial details
- Intigriti's triage team validates the vulnerability

### **Day 2** • Friday

- Organization responds to acknowledge receipt of this information with feedback on its discovery and categorization
- Organization assesses severity and potential impact; preliminary action plan developed
- Development of a detailed mitigation plan, including assembling an on–call team for the weekend
- Prioritization based on severity and potential impact
- Legal implications and responsibilities assessed

**Week 2**

### **Day 3 & 4** • Weekend

- On–call weekend representative notifies ICO of breach (within the legal requirement of 72 hours)

### **Day 5** • Monday

- Communication begins with internal teams, including IT, legal, and management
- Communication plan established for affected stakeholders, such as vendors or third-party service providers

### **Day 6** • Tuesday

- Deployment of any urgent patches or security measures

### **Day 7** • Wednesday

- Continuous monitoring by the organization, with the support of their bug bounty program, for any disruptions or new vulnerabilities

### **Day 9** • Friday

- Coordinated disclosure with affected external parties

**Day 22** • Thursday

- Integration of findings into the organization's cybersecurity strategy

**Day 21** • Wednesday

- Post-incident review: evaluation of lessons learned for future prevention

**Day 19** • Monday

- Implementation of long–term security measures, including training

**Week 4**

**Day 12** • Monday

- Notification to customers about potential impacts

**Day 13** • Tuesday

- Regular updates to maintain transparency
- Continuous monitoring of the affected systems

**Day 14** • Wednesday

- Post-implementation assessment of mitigation efforts

**Day 16** • Friday

- Adjustment of security policies and protocols as necessary

**Week 3**

# Key takeaways

## 1. More urgency is needed for initial response to vulnerability reports

Across sectors, it's clear that many organizations are not responding to critical vulnerabilities quickly enough, leaving them exposed to dangerous cyber threats. In addition to facing potential penalties, a slow response can result in significant security breaches, leading to substantial financial and reputational damage.

## 2. Structured and measurable actions are vital

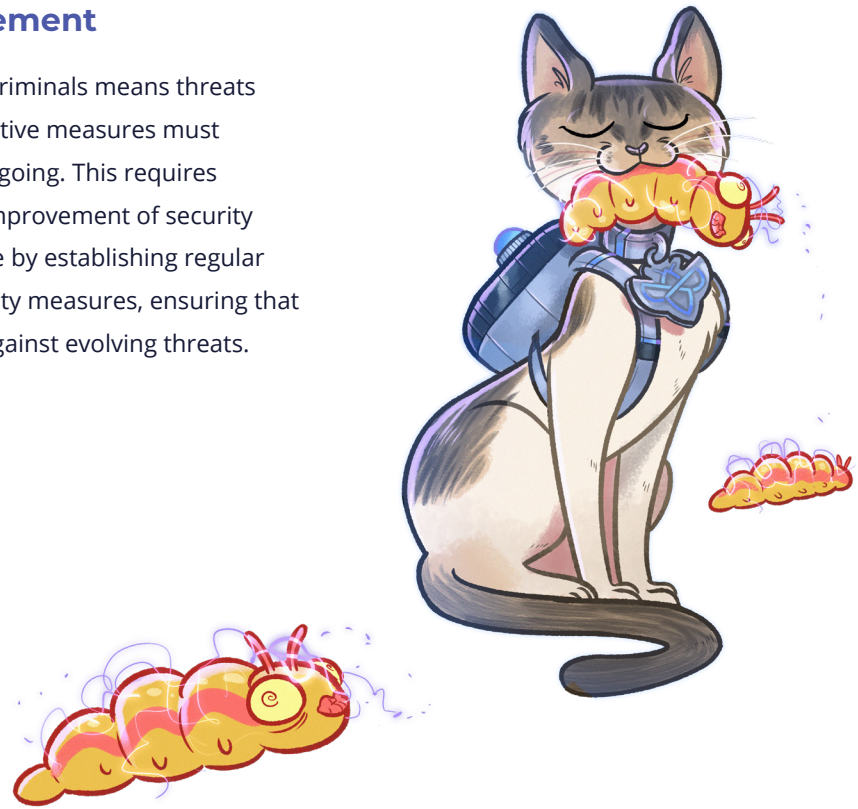
Failing to plan is planning to fail, which is why SLAs are so crucial for protecting against cyber threats. They ensure a structured and measurable approach to fixing vulnerabilities, making the process of acting swiftly and effectively a fundamental part of an organization's security posture.

## 3. Ethical hacking can help

Harnessing the creativity and expertise of ethical hackers can help organizations identify and mitigate vulnerabilities as soon as they surface. By incorporating their findings into SLA frameworks, businesses can respond to threats more efficiently and effectively.

## 4. Constant improvement

The dynamic nature of cybercriminals means threats are always evolving, so protective measures must be similarly adaptable and ongoing. This requires continuous monitoring and improvement of security practices, which SLAs facilitate by establishing regular reviews and updates to security measures, ensuring that businesses remain resilient against evolving threats.



# Fortify your defenses with Intigriti

Connect with the brightest cybersecurity researchers in the world to outmaneuver cybercriminals and stay ahead of the evolving threat landscape. Our easy-to-implement security testing solutions empower you to streamline the vulnerability disclosure process and keep track of submission security statuses in real-time, ensuring a robust defense against emerging threats.

**Ready to outmaneuver cybercriminals with global crowdsourced security?**

Book a meeting today

### Trusted by the world's largest organizations

## What to expect

### Leave the hassle of triaging behind

Our expert 24/7 triage team verifies all reports, saving your team time and ensuring only valid submissions reach you.

### Security assurance

We support your compliance requirements with ISO 27001 and SOC 2 certifications. Our Trust Center provides a live dashboard where you can gain insights into our security and compliance posture in real-time.

### Easy communication

Seamlessly interact with security researchers on the Intigriti platform for updates, questions, and scoping new domains.

### Streamlined processes

Our legal framework ensures swift payment processing in days, outpacing the industry standard by weeks.

### Program oversight

Our dedicated technical customer success team is committed to attracting top-tier security researchers to your program—and keeping them engaged—while conducting regular reviews to ensure sustained momentum post program launch.

Information from Q4/2024. We are constantly growing, so please contact our sales department or see our website for an accurate number.

# Contact us

**Need some help getting started with ethical hackers?**
**Our experts can help you maximize the success of your bug bounty program. Get in touch today to connect with the brightest and most experienced researchers across the globe.**

www.intigriti.com

hello@intigriti.com

Intigriti hackwithintigriti @intigriti Intigriti Intigriti