Onyxia

Key Metrics to Defend Against Threats: **The CISO Perspective**

How hundreds of CISOs assess cyber risk and the impact of their cyber risk strategies.

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Today's Chief Information Security Officers (CISOs) face numerous challenges in quantifying and conveying the business impact of their cybersecurity programs – programs that are essential for keeping both their organizations, and their organizations' customers safe. Across numerous industries, the need to address cyber risk at the board level is growing. The new SEC (Securities and Exchange Commission) regulations for example, require public companies to disclose not only their cybersecurity incidents, but also their risk management strategies and governance policies. To comply with the rules, businesses must perform cyber risk assessments and develop and implement a wide range of cybersecurity policies.

Cybersecurity Management platforms like Onyxia are increasingly important, as they enable CISOs to measure the performance of their risk management strategies and effectively communicate the impact of these cybersecurity initiatives to the board.
To get a greater understanding of how CISOs are measuring and evaluating potential threats, this report speaks directly to CISOs across a wide range of industries. What metrics are they measuring? How are they assessing cyber risk across disparate areas such as incident response, vulnerability patching and phishing simulation, and critically - what is the impact of these cyber risk management strategies?

Methodology

We commissioned a survey of 200 CISOs, 80% from the United States, and 20% from Canada. All CISOs have 3 or more years of experience in their role, and currently work at companies with more than 100 employees. Respondents were split across all industries, with the exclusion of non-profit.

This report was administered online by a third-party global research firm. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during June 2023. The average amount of time spent on the survey was 10 minutes and 50 seconds. The answers to the majority of the non-numerical questions were randomized, in order to prevent order bias in the answers.

Key Findings

1 Cybersecurity Management platforms can simplify the measurement of critical security KPIs for almost all CISOs

89% of CISOs measure the maturity and performance of their security program against all of their critical KPIs at least once each quarter, and more than half of CISOs measure them all monthly. Cybersecurity Management Platforms, are relatively new solutions, in direct response to this growing need. The right technology can simplify and automate a task that is heavily manual for today's CISOs.

2 CISOs have dangerously low expectations for incident detection

33% of CISOs are not working towards a same-day Mean Time to Detect (MTTD), and do not have an SLA to start working on mitigating risk within 8 hours of a breach. In addition, the average SLA for patching and resolving critical vulnerabilities is 16.3 days. Attackers have a perfect landscape to launch attacks and deepen their foothold.

3 The majority of CISOs target a MTTR of one day or less

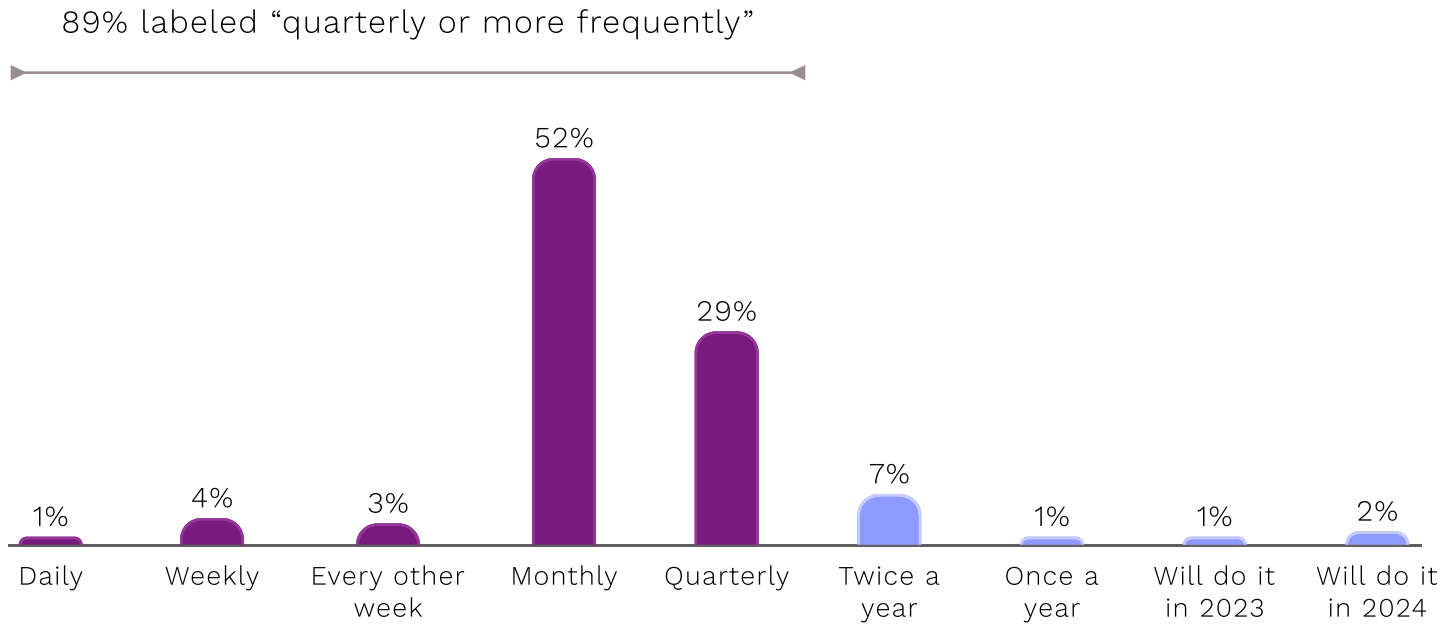
On average, the KPI for Mean Time to Respond (MTTR) is 9 hours. However, while many have the conception that the Financial Services industry is ahead of the curve in security, their average SLA for MTTR is actually higher, at 9.3 hours. This makes them less mature than average, and far less mature than the IT industry, who have a target MTTR of 7.4 hours.

Survey Report Findings

Frequency of Measuring Security Program Maturity and Performance KPIs

The vast majority (89%) of CISOs measure the maturity and performance of their security program of all critical KPIs at least once each quarter. In more than half of cases (52%), CISOs measure all their KPIs monthly. Just 3% do not measure the maturity and performance of their program, but have plans to either this year or in the next 12 months.

Without a Cybersecurity Management platform in place to perform this critical task, measurement of KPIs related to maturity and performance have to be completed manually, taking resources away from performing critical security strategy. In contrast, with a CPM solution in place, CISOs can take stock daily if they choose, giving them full transparency at all times.

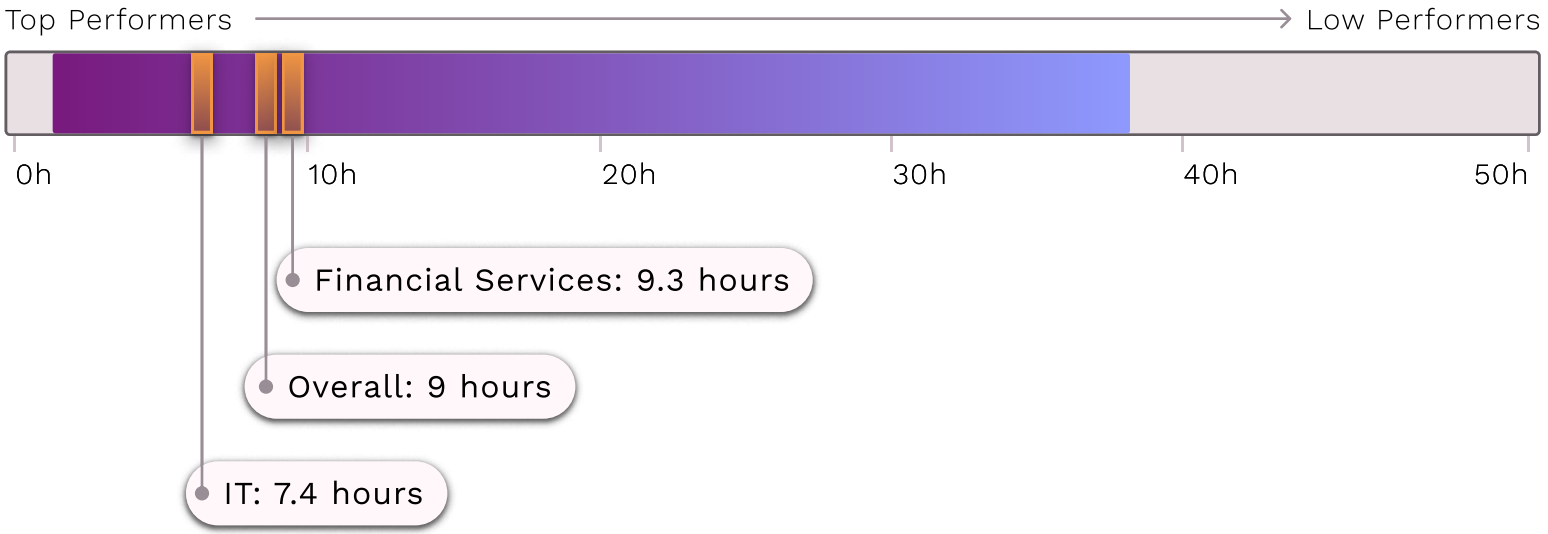


Target SLA for Responding to Security Incidents (MTTR)

Mean Time to Respond (MTTR) is an important KPI for all security teams, as the longer the dwell time of an attack, the more catastrophic its impact. Our respondents indicate that the average target SLA for MTTR, or more simply - how quickly they want to respond to security incidents, is 9 hours.

Just 8% say that they can offer an SLA of 2-3 hours, and in more than a quarter of cases, CISOs have a target SLA of more than 10 hours to respond to an incident.
We broke down the data by industry, and found that Financial Services have an average target for MTTR of 9.3, almost 2 hours longer than IT.

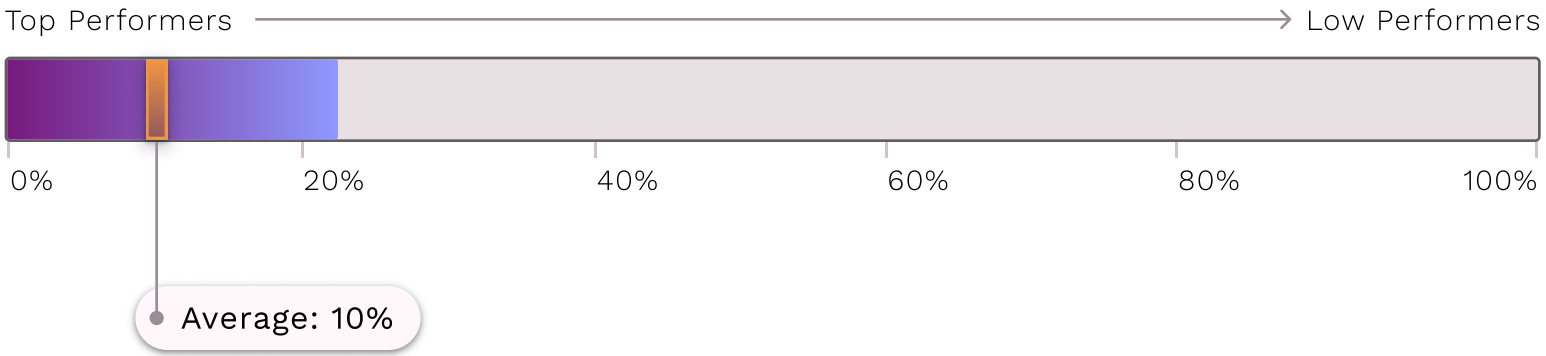
Average SLAs



Acceptable percentage of incidents that exceed the SLA for MTTR

It's an unfortunate truth that the sheer number of alerts means that some security incidents will not be responded to within the SLA. We asked CISOs what percentage of incidents they hold as acceptable to exceed the SLA, and found that on average, this is 10%. Seven percent (7%) of CISOs say that 20% of incidents do not meet their target SLA for MTTR.

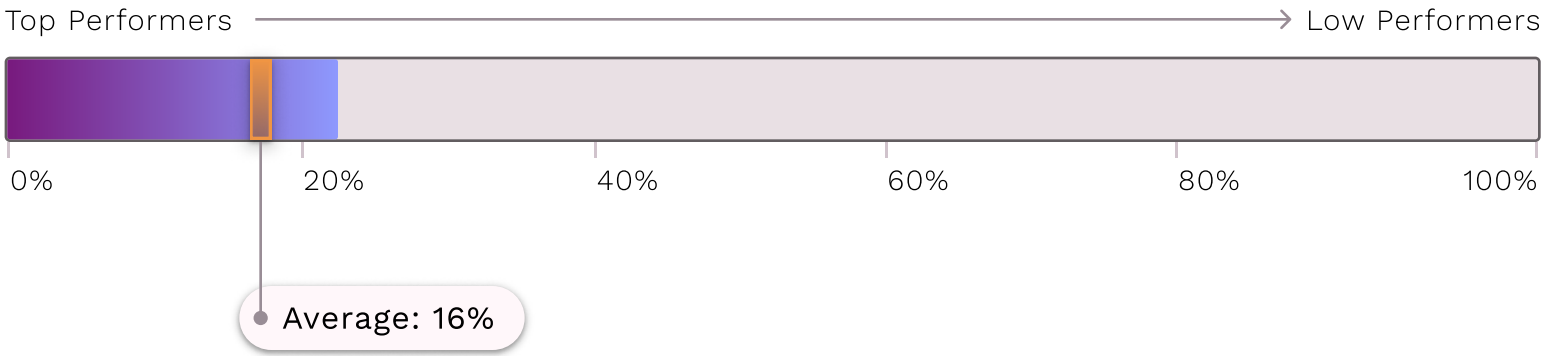
Average acceptable percentage



Acceptable False Positive Rate for SOC Incidents

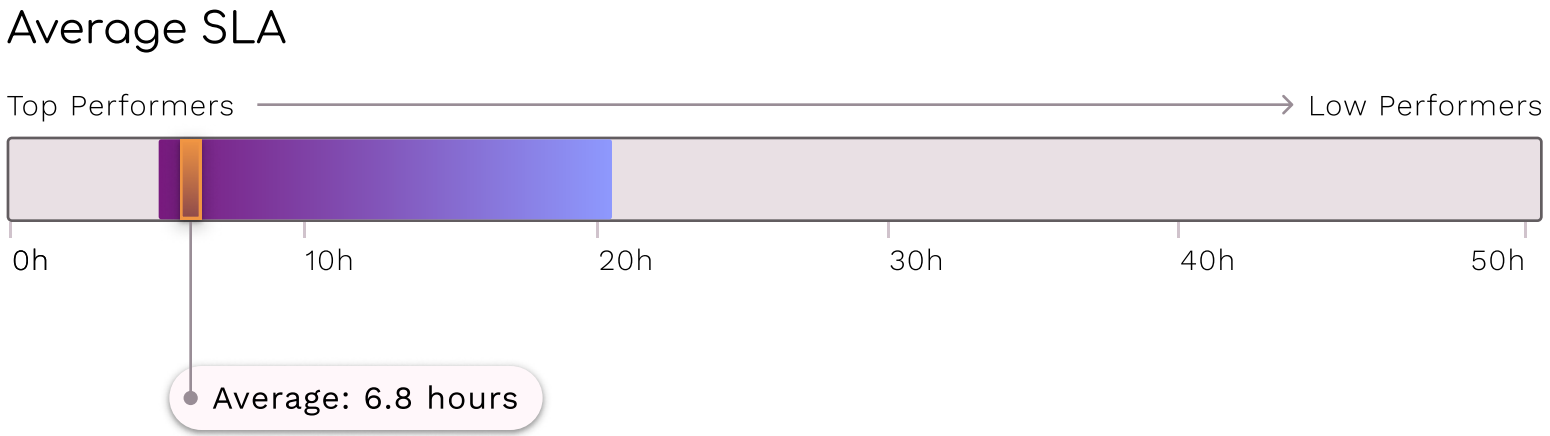
For alerts to be comprehensive, a certain degree of false positives are expected. However, we were surprised to see how many false positives CISOs accept in their day-to-day SOC operations. The average acceptable false positive rate for SOC incidents is 16%.
Twenty six percent (26%) of CISOs say their acceptable rate of false positives is under 5%, while for 28% of CISOs, a rate that's more than 20% would fall into the acceptable range. That would mean 1 in 5 incidents are false positives.

Average acceptable rate



SLA for Mean Time to Detect (MTTD) for Security Incidents

The average SLA for mean time to detect (MTTD) for security incidents is 6.8 hours. Two-thirds of CISOs are targeting same-day detection (within 8 hours), which is great to see. However, for the remaining 33%, time is being wasted which could give attackers a chance to establish a deeper foothold.

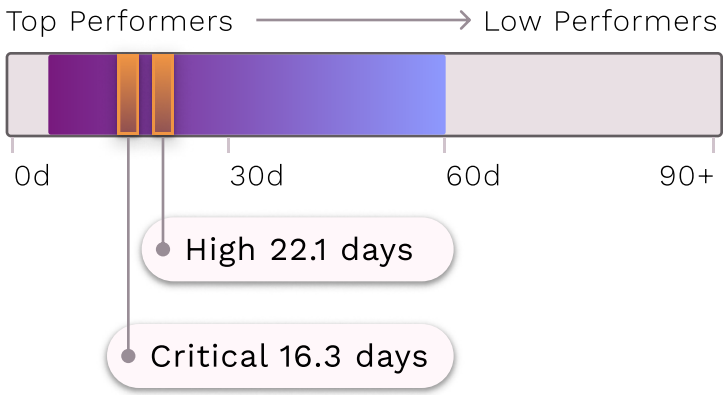


SLA for Patching/Resolving Vulnerabilities

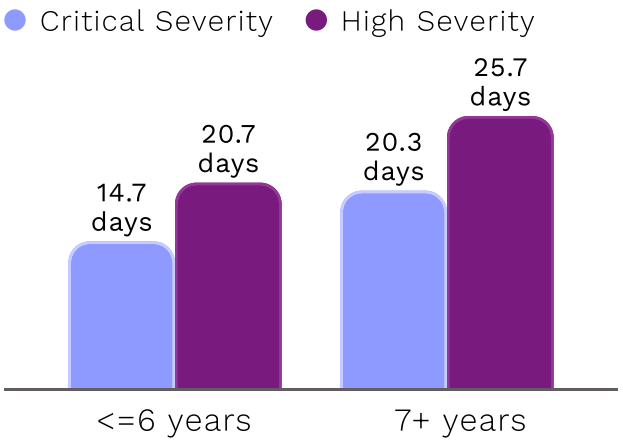
Patching vulnerabilities is a real bear for the security industry. The average SLA for patching or resolving critical severity vulnerabilities is 16.3 days. The average SLA for patching/resolving high-severity vulnerabilities is even longer, at 22.1 days. This timeframe leaves the door wide open for attackers to abuse vulnerabilities to attack organizations. We can see in the data that critical severity vulnerabilities are given priority, and therefore 75% are resolved within 21 days, compared with 48% of those that are high severity.

We looked at those who had more and fewer than 6 years of experience as a CISO, to see whether this had an impact on how quickly vulnerabilities can be resolved. Interestingly, those with more experience actually say it takes longer to resolve issues. This could be because from their senior vantage point, they are more realistic when it comes to the time patching and vulnerability management can take.

Average SLA by Severity



Average SLA by Seniority

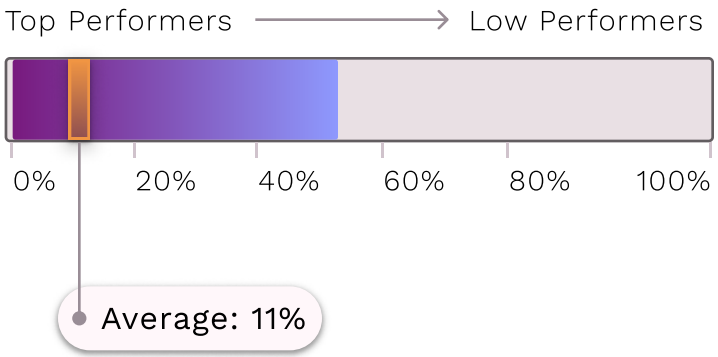


SLA for Patching/Resolving Vulnerabilities

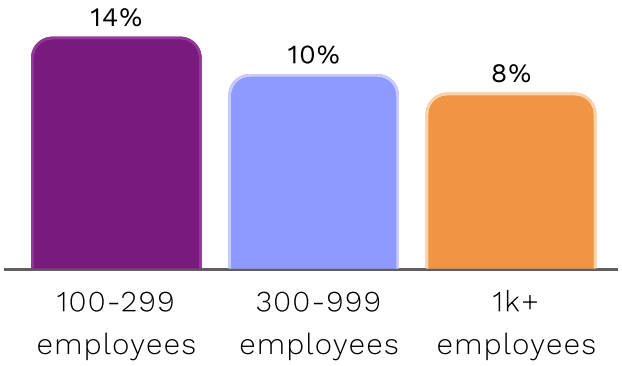
The majority of CISOs accept that 10% of high or critical vulnerabilities will not be patched or resolved on time. On average, CISOs feel 11% of vulnerabilities unresolved or patched is an acceptable number, similar to the 10% we say in Figure 4, who accept that not all incidents will receive a response within the SLA timeframe or to meet a specific KPI.

Breaking down this data by company size, larger companies have a lower acceptable percentage of high/critical vulnerabilities that remain unpatched. For smaller companies with up to 300 employees it is 14% on average, for medium companies with 300-999 employees it is 10%, and for big companies with 1K+ employees it is only 8%. Larger companies often have dedicated teams to resolve vulnerabilities, so they can afford to make tighter expectations around SLAs and KPIs.

Acceptable percentage left unresolved



Average acceptable percentage, by company size

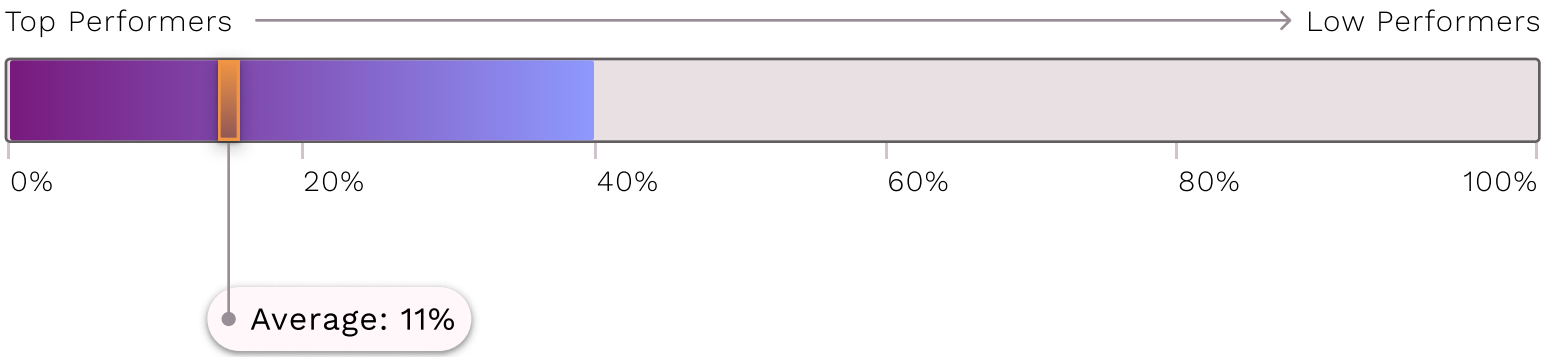


Acceptable Percentage of Unpatched Vulnerabilities with a Public Exploit

When a vulnerability has a public exploit, the risk is extremely high. Despite this, we can still see here that a similar and significant percentage of CISOs (11%) still accept these exploits remaining unresolved and patched within their SLA timeframe.

We would have expected to see this number a lot lower, suggesting that CISOs don't have the technology in place to resolve this issue and patch more effectively, even when the risk is extremely high.

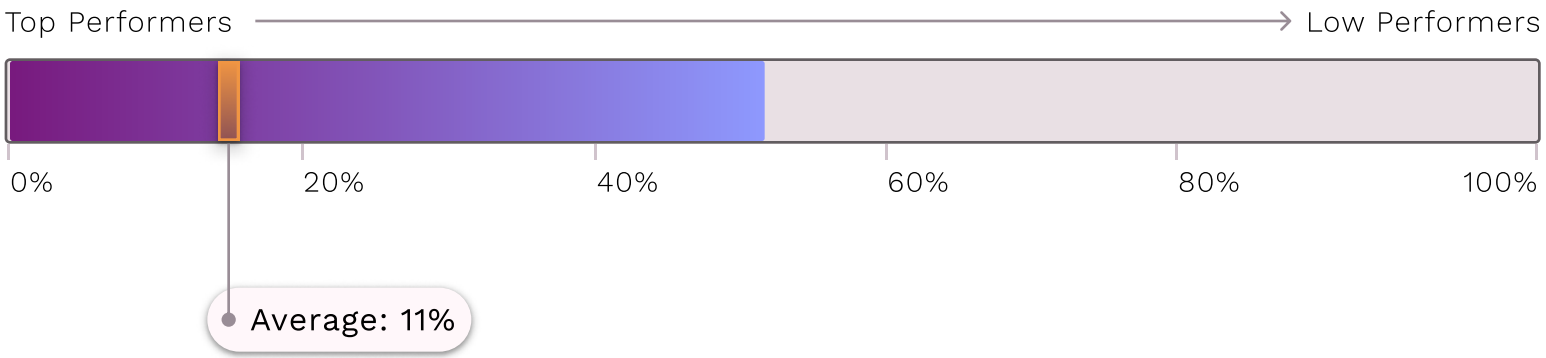
Average acceptable percentage



Acceptable Percentage of Assets with Unpatched Vulnerabilities

In a similar vein to what we've discussed so far, the average acceptable percentage of assets with unpatched vulnerabilities is also 11%.

In 10% of cases, CISOs are accepting between 21%-40% of assets with unpatched vulnerabilities, opening their organizations, and their customers, up to risk.

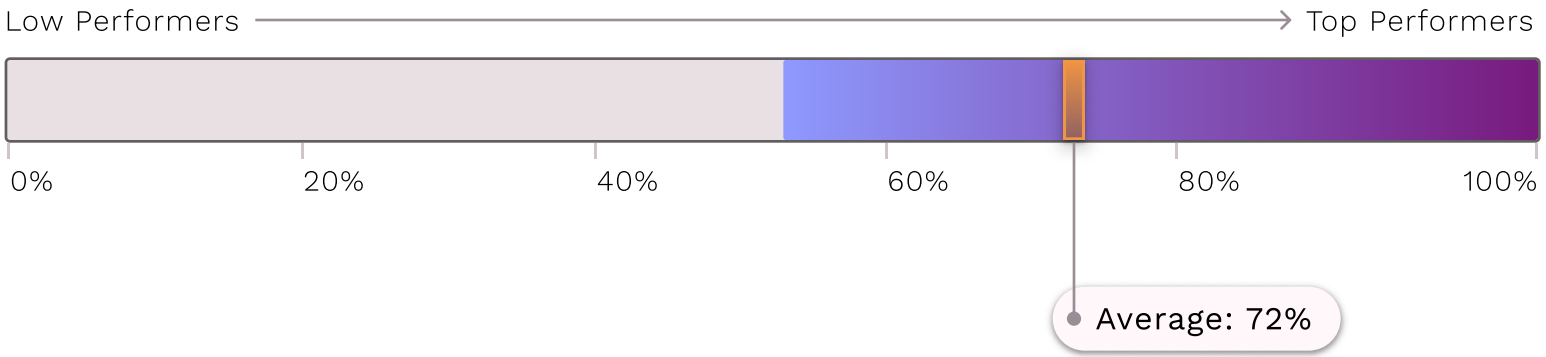


Target Reporting Rate for Phishing Simulations

CISOs often set a KPI or SLA to see what percentage of users report clicking on or finding a suspicious link during a phishing simulation. The data shows that CISOs on average expect the reporting rate to be 72%. This may depend on whether a company has systems such as one-click reporting set up to make disclosure easier.

In 15% of cases, CISOs expect the reporting rate to be 90% or higher, and 10% of CISOs set an SLA or KPI for under 40%.

Average target reporting rate

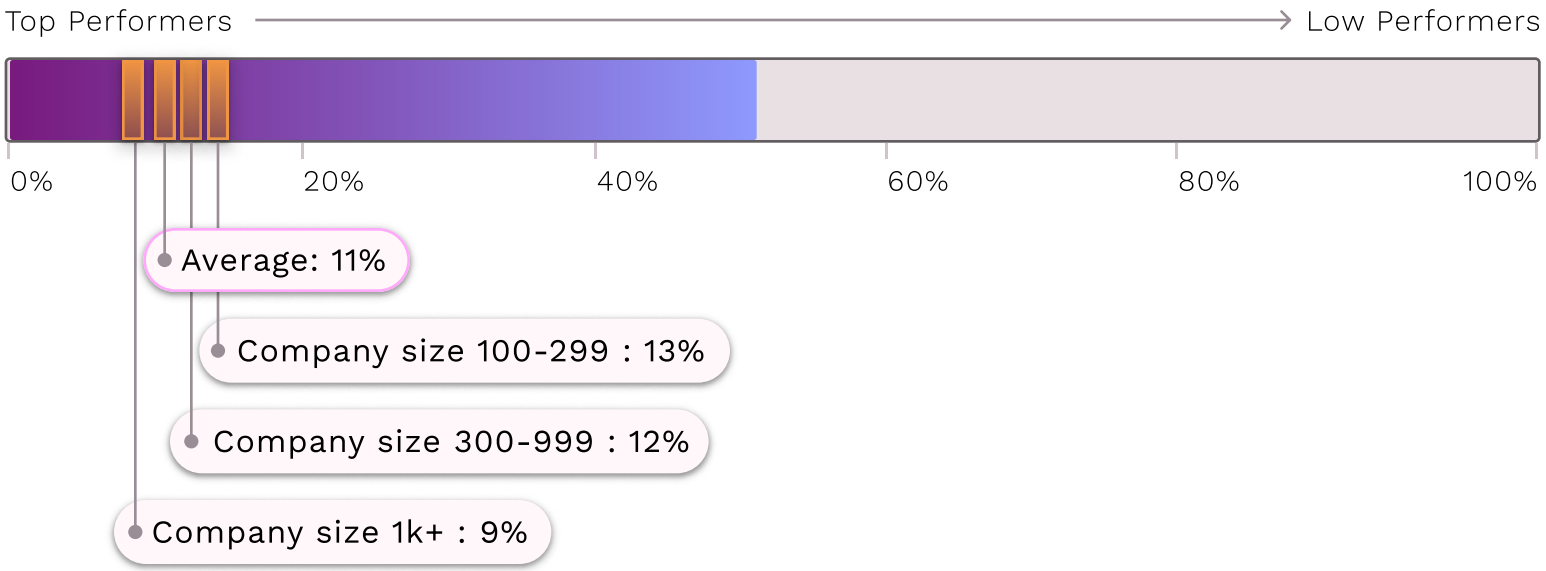


Acceptable Click Rate Percentage on a “Malicious” Link During a Phishing Simulation

CISOs on average believe an acceptable rate of clicking on a phishing simulation is 11%. This paints a picture of very realistic security leaders who recognize the threat of phishing in their environment. Seventy-eight (78%) of CISOs set their target for those who fall for phishing simulations between 5%-20%.

It’s also important to consider that phishing simulations who trick no-one also teach no-one. Security awareness programs that have a 0% click rate are not the goal, as they may just be too easy, and we know that phishing scams do work in the real world.

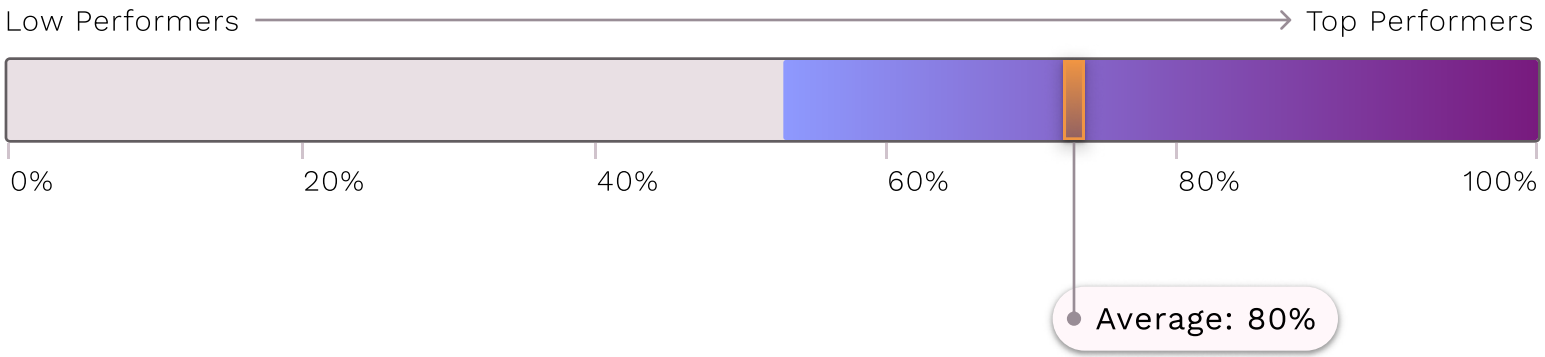
Average acceptable percentage



Acceptable Percentage of Users who Successfully Passed Security Awareness Training

Many U.S. companies need to implement security awareness training in order to remain compliant with various regulations. CISOs have a high expectation that users will take and pass security awareness training. On average they believe that 80% should be security awareness trained. Twenty-seven percent (27%) of CISOs think this number should be 90%.

Average acceptable percentage



Demographics

Industry, Seniority, Company Size, and Country

Industry:

Information Technology	Energy & Utilities	Banking	Insurance
Financial Services	Health & Pharma	Education	Travel & Hospitality
Manufacturing	Construction	Professional Services	Food
Retail & eCommerce	Media	Transport & Logistics	

Company Size

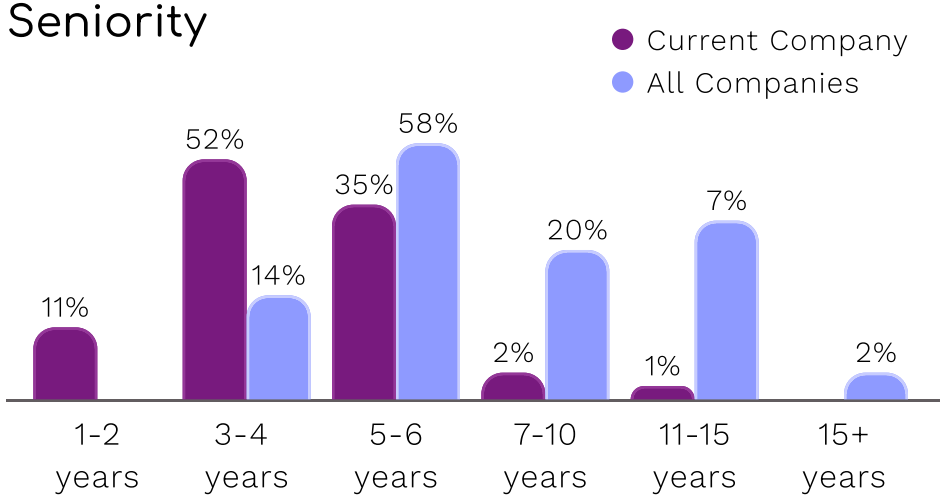
100-10k+

Country

United States: 80%

Canada: 20%

Seniority



About Onyxia

Onyxia Cyber is on a mission to help Chief Information Security Officers (CISOs) and security leaders continuously strengthen and gain a complete view of their cybersecurity programs. Its AI-powered Cybersecurity Management Platform provides real-time security assessment and benchmarking, full visibility into program performance, and streamlined board reporting. The platform allows CISOs to make data-driven decisions through actionable insights based on their organization's internal environment, external intelligence, and industry threats. With Onyxia, CISOs gain a simplified way to convey the value of the security program and align their security initiatives with their organizational goals.

Book a Demo

For more information, please visit us: