binalyze!

A Binalyze research report

The State of Cybersecurity Investigations 2025:

How Cyber Scene Investigators can turn the tide against attackers' sense of impunity

Findings are based on a survey of 200 US CISOs and others with sole responsibility for IT cybersecurity decision-making at enterprises with 500 or more employees. Research was performed in September 2025.

Executive summary

Cyber attackers think they're winning.

They are holding our cities to ransom; disrupting our courts and judiciary; and stealing the data of innocent patients. Their impact is felt from critical national infrastructure to food supply to manufacturing. As AI democratizes cyberattacks, the attackers are getting bolder: even boasting to global media about their successes.

Help isn't coming. Governments can only react to new threats, and move slowly when they aren't paralyzed by political maneuvering. Even then, legislation to improve security cannot and will not prevent breaches, and many governments are reduced to sending advice letters instead of taking concrete action.

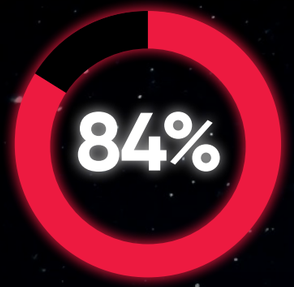
Against this backdrop, the odds of a successful cyberattack are no longer up for debate. The question is not if. It's when. With an enemy no longer at the gates but scaling the walls, cybersecurity is at a crisis point. As IT environments and attack surfaces rapidly expand with new technologies, security teams have a critical role. Not only defending against attacks, but preventing them from causing crippling damage and turning the tide against attackers.

Cyber Scene Investigation plays a vital role. Understanding attacks and attackers is the key to victory. Rapid, forensic investigation is critical to stopping attacks before they do serious damage; informing stakeholders to protect the organization's reputation; and sharing intelligence so other organizations avoid falling victim.

To understand how effective organizations' Cyber Scene Investigation strategies are, Binalyze surveyed 200 US CISOs. We wanted to understand how organizations are reacting to the seeming inevitability of cyberattacks. Whether they have crisis management frameworks in place to resist and repel invaders. Whether their CSI teams can act with the speed and depth needed to provide complete, actionable insights. And whether a lack of skills is harming teams' effectiveness.

We found gaping breaches in enterprises' crisis management frameworks, with most organizations failing to learn the right lessons from cyberattacks. This in turn means increased financial and reputational damage, and not only from regulatory action or denied insurance payouts. Delayed investigations cost hundreds of thousands of dollars each time, while a lack of visibility creates inconclusive investigations that again cost millions. And all the while, CSI teams are over-worked and at risk of burnout.

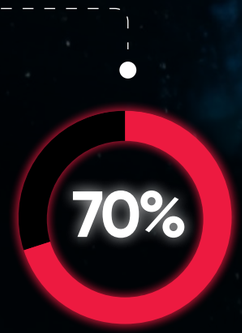
However, there is light at the end of the tunnel. Enterprises recognize the value of rapid, forensic investigation. And with the right tools and approach they can turn defense into offense: rooting out potential threats and weaknesses and slamming the gate on attackers.



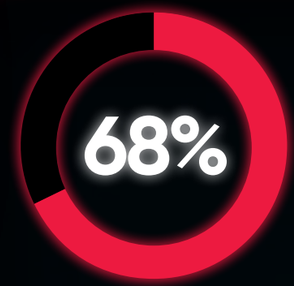
Failing to learn from the inevitable:

84% of CISOs say a successful cyberattack is "inevitable", but **65%** admit their organizations "haven't always" learned the right lessons. **75% of CISOs** say once a cyberattack has happened there's "no guarantee" that the exact same attack won't succeed again.

Crisis management frameworks in crisis:



And **70%** have struggled to remediate or recover from an attack in the past year.



Lack of clarity costs enterprises dearly:

68% of CISOs have "inaccurately reported" a breach to regulators because of a lack of forensic clarity, and **74%** have claimed less insurance than entitled to because of a lack of confidence in the claim.

Each hour of delay in responding to a cyberattack costs $114,000

While a lack of clarity in investigations costs enterprises on average **$1.1 million.**

CSI skills are at a premium:

Despite having on average 18 skilled investigators in their team, **90% of CISOs** say a lack of skills has hampered investigations.

Part one

A golden age for attackers?

To cyber attackers, this can feel like a golden age. AI has opened new opportunities, allowing them to iterate and distribute attacks at previously unimagined scales, with AI-powered cyberattacks now an accepted part of risk taxonomy. At the same time, attack surfaces are growing while cybersecurity itself becomes increasingly complex.

Facing new attack vectors such as deepfake-powered phishing; newly notorious groups such as Scattered Spider; and new national and global regulation such as DORA, security teams accept that the dam cannot hold. Successful cyberattacks are no longer a risk. They are an inevitability.

84% of CISOs say:

"Organizations will inevitably suffer from a successful cyberattack"

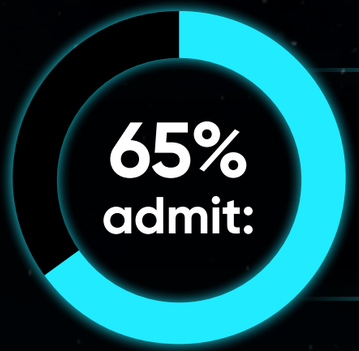
This creates a delicate balancing act for security teams. Prevention is still essential, to ensure that inevitable attacks are isolated incidents instead of a constant flood. But when the inevitable happens, effective response is critical to understanding the attack, preventing damage, and ideally turning the tables on attackers.

79% of organizations' IT budgets are balanced in favor of prevention; 12% in favor of response (and 9% 50/50)

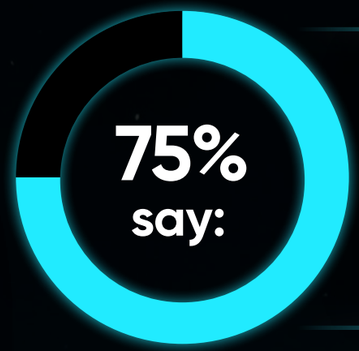
On average, budgets have a 2:1 ratio towards prevention ($3.02 million on prevention, and $1.54m on response).

Cyber Scene Investigation is a crucial element of this response. In the short term, it allows the organization to triage attacks; isolate compromised assets; and report accurately to stakeholders such as the board, regulators and insurers. In the long term, understanding and sharing intelligence is the only way to clip attackers' wings. But without the right resources, focused in the right direction, this cannot happen.

What the CISO's say:



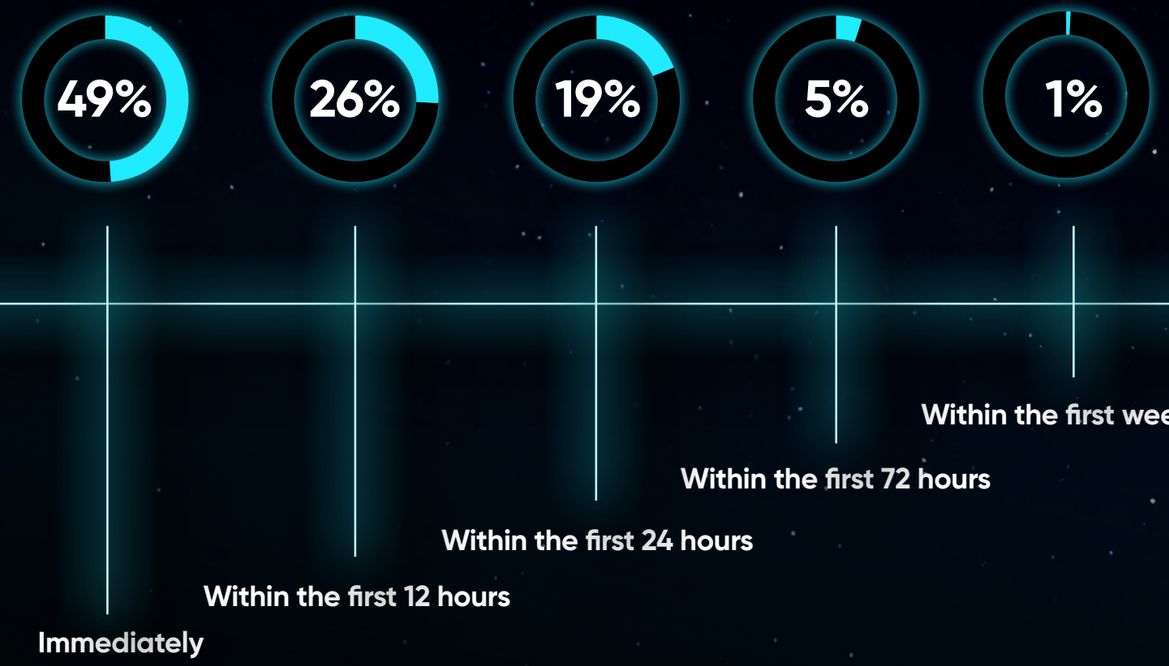
their organizations "haven't always" learned the right lesson from cyberattacks.



once a cyberattack has happened there's "no guarantee" that the exact same attack won't succeed again.

CISOs are under no illusions about the importance of in-depth, forensic investigation, and how it represents the difference between taking control or remaining a victim. They also know that speed is of the essence: the faster forensics come into play, the quicker the organization can not only recover but find ways to make attacker's lives harder.

How soon after an attack should forensics come into play?



Mean time to bring forensics into action: 8.6 hours.

CISOs recognize swift, forensic investigation's value as a defensive weapon. But it doesn't need to be solely reactive. Deployed offensively, forensic investigations can form a vital countermeasure: hunting threats and identifying potential vulnerabilities before attackers have the chance to exploit them.

Used correctly, investigation is both an essential element of a crisis management framework, and a weapon to help prevent crises in the first place.

Part two

The crisis management framework crisis

When the worst happens, a crisis management framework makes the difference between a focused, organized reaction and blind chaos.

However, rapid evolution means many organizations can find their own framework has been made obsolete. The result is a lack of confidence in the organization's posture.

Only 40% of CISO's have "complete confidence" in their organization's crisis management framework.

At most 37% of enterprises can guarantee they have all the pieces of a comprehensive crisis management framework for cyberattacks in place.

The elements of a cyberattack crisis management framework:

At its most basic, the cyberattack victim needs to answer the basic questions. Does the attacker still have access? How did they get in? Was data stolen? And if so, which data? There's no right answer, but it will form the basis of every action taken. Yet at most, only half of CISOs can confidently answer them all.

At most 50% of CISOs can answer ALL of these cyberattack questions with complete confidence:

Being able to answer these questions with confidence should be every organization's priority. From there they can move to the ability to investigate attacks in detail; having detailed action plans; having a clearly defined crisis management team in place; and the other factors that determine a framework's success and help enterprises perfect their defensive stance.

Crucial cybersecurity elements of a crisis management framework:

The ability to investigate every potential cyberattack in detail.

44% of CISOs have "complete confidence" they can do this.

The ability to present stakeholders with relevant information in a timely manner.

44%

Having detailed action plans for every form of cyber incident that could reasonably affect the organization.

37%

Having rigorous review processes in place to prevent future crises.

45%

Having a crisis management team in place, with defined roles.

46%

Conversely, without these elements in place it becomes harder to effectively remediate and recover from attacks. If we look specifically at CSI, we can see the impact this has.

The impact of investigation:

Enterprises already investigate nine cyberattacks a year in depth. These are not spaced evenly throughout the year (i.e., every five to six weeks), suggesting waves of attacks that can catch defenders off guard and increase the demands on CSI teams.

Enterprises investigate nine cyberattacks in depth per year

The most recent investigation was 10.5 weeks ago

Ideally, enterprises could investigate every potential cyberattack in detail, building a vast intelligence library. In reality, most have to choose. Between those attacks that remain undetected, and those the organization doesn't have the resources to address, only a minority are acted upon.

On average, 64% of attacks are not acted upon.

CISOs believe:

40% of attacks on their organizations go undetected

CISOs say:

39% of identified or suspected attacks are not acted upon

Ultimately, the less an organization understands an attack, the harder it will be to recover from it, and the harder it will be to share any intelligence or insight.

70% of organizations have struggled
to effectively remediate and recover from an attack in the past year because they did not understand the root cause, scope, and impact.

64% of CISOs have struggled
to explain the details, impact, or significance of a cyber breach to the board.

This lack of understanding has wide-spreading ramifications. Cyber insurers will deny payouts if an attack victim cannot prove it had all relevant controls in place. Regulators demanding compliance want to see organizations have taken appropriate action, and uncovered and shared the appropriate information, at every step. Even if the organization has acted appropriately, a lack of evidence can undo all their efforts.

56% of CISOs' organizations have been denied a cyber insurance payout.

61% of CISOs' organizations have been punished by regulators because of a security breach.

68% of CISOs have seen refused cyber insurance payouts or regulatory punishment that were unjustified, but happened because the victim couldn't prove otherwise.

Building a comprehensive crisis management framework means taking control of investigations. And this means improving their speed, depth, and scope.

Part three

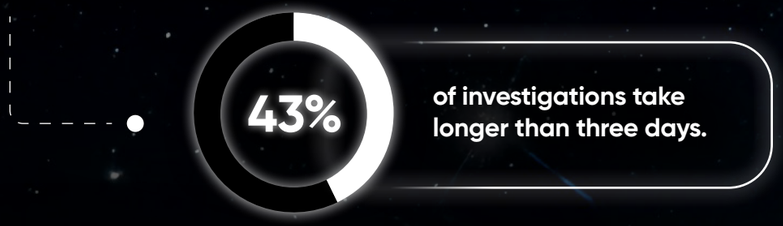
Light speed and black holes

As the backbone of a crisis management framework, successful investigations depend on two factors. First, speed. Every minute is an opportunity for attackers to do more damage or hide their tracks, or for organizations to build a complete picture, update stakeholders, and warn the wider community of new threats.

Second, breadth and depth. Vast modern IT environments create black holes of information, from which no insight can easily escape. Shining a light into these and exposing previously hidden data can make the difference between a successful investigation and one that cannot satisfy stakeholders.

Travel at light speed:

The average cyberattack investigation produces results 8.5 days after the attack is discovered.



Investigations happen quickly, but there is still room for improvement. Every day spent is a day where the organization cannot resume full operations with confidence; where trust in the organization can falter; and where attackers could be spreading their own misinformation to the public.

88% of CISOs agree that faster investigations would reduce the cost of breaches. And the costs of a delayed response quickly add up to millions.

CISOs calculate that each hour of delay in responding to a known cyberattack costs $114,000.

If we consider the average time to engage forensics, this translates to **$980,000 per attack.**

If we consider just the number of attacks investigated each year, this translates to **$9 million.**

There are two elements that will accelerate investigations. The first is the right tools: a platform that will enable investigations to be measured in hours, not days. The second is the ability to be proactive. The more organizations control investigations, the faster they can begin them, the faster they can act on the results.

Why have enterprises triggered investigations in the past 12 months?

53% proactively, based on threat intelligence

50% proactively, based on internal intelligence

47% reactively, based on internal alerts

45% reactively, based on alerts from third-party SOCs

43% reactively, when required to by auditors, regulators, or insurers

41% reactively, based on notification of a potential incident from third parties (e.g., law enforcement)

Black holes and revelations

75% of CISOs feel they are missing "key information" every time there is a breach.

72% say that investigations are, by necessity, based on "incomplete" information.

72% have begun investigations without knowing where to look first.

68% have been forced to close investigations without finding the root cause.

Always-expanding IT environments and attack surfaces are stifling investigations. CSI teams cannot limit themselves to only looking at individual pieces of evidence. But unlike the real world, there is no natural limit to a cybercrime scene. Any black holes within an organization's environment can hide crucial evidence, resulting in investigations that lack clarity. And this lack of clarity will have very real consequences for the organization.

A lack of clarity in investigations costs enterprises on average $1.1 million.

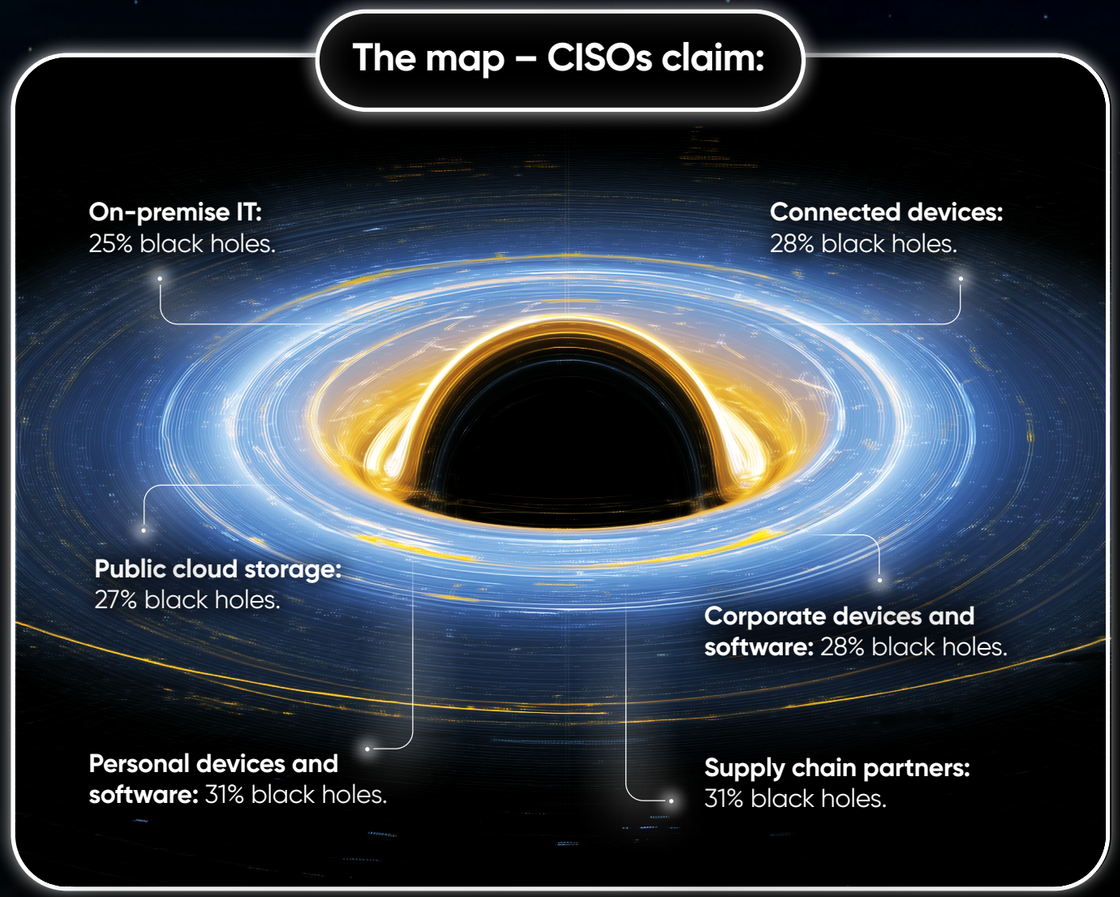
68% of CISOs' organizations have "inaccurately reported" a breach to regulators because a lack of forensic clarity.

74% have claimed smaller amounts on insurance than they might have been entitled to because of a lack of confidence in the claim's strength.

Solving this demands visibility. Security teams need to understand their entire IT environment: including what they have visibility into, and where these black holes exist. Armed with this "map" of their infrastructure and tools that will allow them to shine a light into black holes, they can begin exploring and prizing insight from the darkness.

The map of IT environment black holes

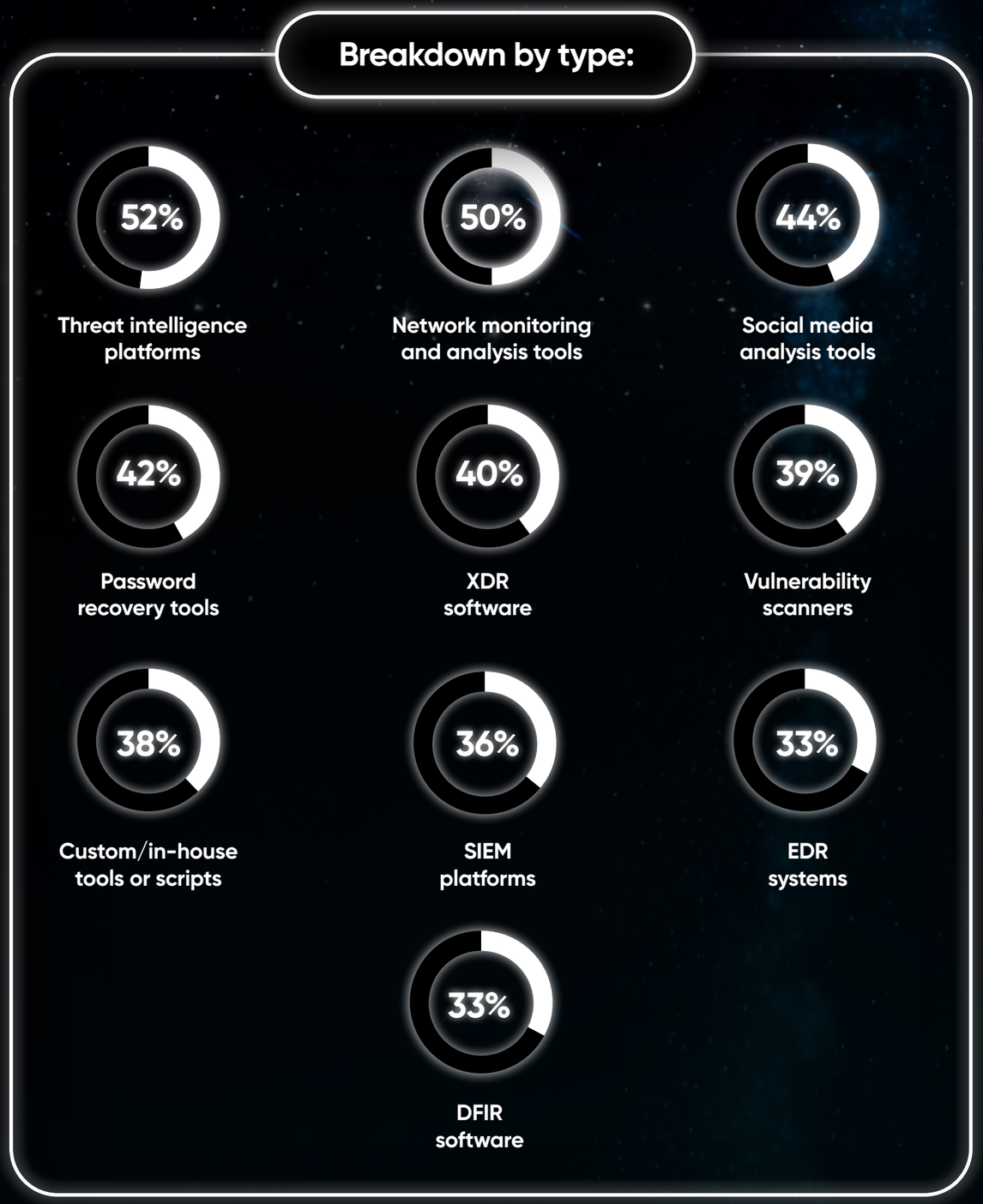
On average, CISOs claim to have visibility over 57% of their organization's IT environment at any one time.



Another potential contributing factor to a lack of clarity in investigations is the number of tools used. CSI teams have a wealth of investigation tools at their disposal. But these need to be used in concert, to avoid conflicting evidence; incomplete or potentially inaccurate data; and wasting time.

Enterprises use on average 11 tools to investigate cyberattacks.

Breakdown by type:



Part four

Avoiding CSI team burn-out

The average enterprise has 18 skilled cyber investigators on staff.

To accelerate investigations and shine light into black holes of information, CSI teams need skilled investigators. This isn't only a matter of having enough people, with the right skills. The question is whether this is enough. And CISOs say it isn't.

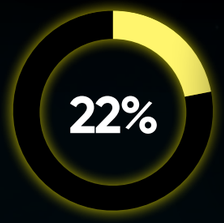
Only 32% of CISOs have all of the skills they need to perform investigations completely in-house.

CISOs spend **on average 5.5%** of their budget outsourcing cyber investigations.

- An average of **$252,000**
- Reaching the level of investigation skills they need would add **14% to CISOs' budgets**
- An average of **$625,000**

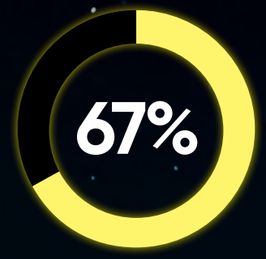
However, the impact of a lack of skills goes much further than adding to costs via outsourcing or additional hires. It has a direct, detrimental impact on investigations themselves.

90% of CISOs say a lack of skills has hampered their cyber investigations in the past five years.

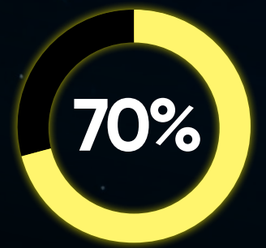


say it has done so every time – the equivalent of 45 investigations.

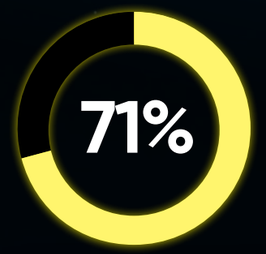
of enterprises are "too under-staffed and under-skilled" to perform investigations.



have had to delay or give up investigating a breach because of a lack of skilled investigators.



had to do so because investigators were needed elsewhere.

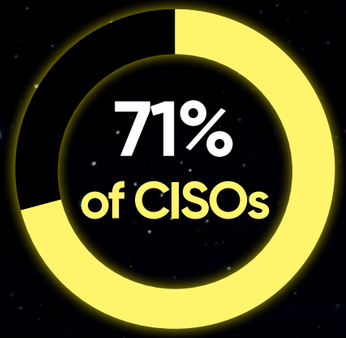


of enterprises have "delegated" investigations to employees without the necessary skills.

The business is not the only potential victim of skills shortages. As investigators find themselves under pressure, performance suffers, and the risk of burnout and shrinking teams increases.

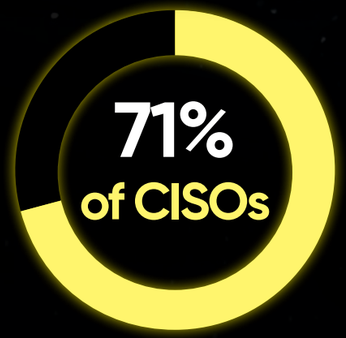
This lack of skills can mean investigations are delayed; return less-trustworthy results; or end up abandoned altogether. Organizations can try and save their CSI teams' time by "delegating" to colleagues who lack some or all of the necessary skills. But without careful support, this will again result in compromised investigations.

Ultimately this means the organization cannot learn the right lessons from attacks, and the goal of a crisis management framework drifts further away.



worry that their skilled investigators are over-worked and at risk of burnout.

If this is not addressed, the result will be a slow whittling down of skills, as experienced investigators leave, their hard-earned skills become correspondingly rarer and more expensive, and organizations are ever-more exposed.



have had investigators resign or take time away because of burnout.

68% of CISOs worry that their existing skilled investigators are looking for other jobs.

If there is no way to bolster numbers, CSI teams need the tools that will make them more effective. Allowing them to perform their most vital tasks at full capacity, while giving other team members the capability to take on simpler workloads.

Conclusion: From Crisis to Capability

Cyberattacks are no longer the exception, they're the expectation. Cybersecurity leaders know prevention alone won't hold the line. The difference is how prepared they'll be when an attack does strike. What defines resilience today is how quickly and intelligently you investigate once defences are breached.

This report highlights the cost of delay and disjointed response to attacks. As such, CISOs must move beyond reactive defence and embed investigation at the heart of their security strategy. The goal is not more tools, but the right ones: platforms that unify visibility, accelerate response, and allow teams to illuminate every corner of their IT environment.

The benefits extend beyond the security team. Fast, transparent investigation builds confidence among executives, auditors, regulators, and insurers. It also transforms every incident into a learning opportunity, strengthening systems, processes, and people for the next challenge.

With the right technology and leadership, investigation becomes a driver of resilience. The next attack may be inevitable, but with clarity, speed, and insight, its impact doesn't have to be.

To learn more about how modern investigation solutions balance AI-powered speed with human-driven insight, visit: binalyze.ai

Methodology

Findings are based on a survey of 200 US CISOs and others with sole responsibility for IT cybersecurity decision-making at enterprises with 500 or more employees. Research was performed in September 2025.

binalyze!

A Binalyze research report

The State of Cybersecurity Investigations 2025:

How Cyber Scene Investigators can turn the tide against attackers' sense of impunity

Findings are based on a survey of 200 US CISOs and others with sole responsibility for IT cybersecurity decision-making at enterprises with 500 or more employees. Research was performed in September 2025.