HOXHUNT

Human Cyber-Risk Report

CRITICAL INFRASTUCTURE

THE HUMAN RISK REPORT SERIES · 2023

Contents

Introduction: Complexity of critical infrastructure

This report on human risk in the critical infrastructure sector comes from **an analysis of over 15 million phishing simulations and real email attacks reported in 2022 by 1.6 million people** participating in a security behavior change program. Over 65% of active participants in this behavior change program detect and report real malicious email attacks within a year of commencing training. The fact that 2/3 of people are detecting a real attack is one of the most impactful measures of true security behavior change that we know to have been recorded. Real threat detection is a key value driver in transforming security awareness programs into human risk management.

These findings reveal valuable insights into the state of human risk. And, importantly, how human cyber-risk can be demonstrably mitigated by a robust behavior change program in the critical infrastructure sector, which the White House singled out as the top strategic pillar in its Cybersecurity Strategy document [1].

Energy & Utilities companies are emphasized in this analysis, which compares critical infrastructure results against the global average of all sectors. According to CISA, critical infrastructure includes 16 sectors [2].

“

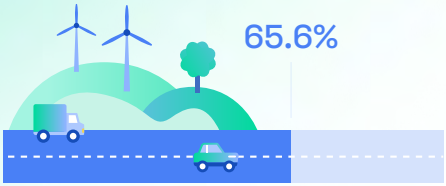
… much work remains to ensure the security and resilience of our critical infrastructure in light of complex threats and increasing geopolitical tension… We need to normalize cyber risks for the general public with the recognition that cyber-attacks are a reality for the foreseeable future. We cannot completely prevent attacks from happening, but we can minimize their impact by building resilience into our infrastructure and into our society. We need to look no further than our Ukrainian partners for an example of the power of societal resilience.”

JEN EASTERLY, CISA DIRECTOR

Key Takeaways

51%

Resilience ratio (success rate / failure rate) in critical infrastructure is 51% higher than the global industry average: 10.9 for critical infrastructure vs. 7.2 for global average.



65.6%

Training boosts measurable human threat intelligence: Of active security behavior change program participants, 65.6% detected and reported a real threat in one year

20%

Resilience velocity is 20% higher in critical infrastructure (organizational real threat detection rates reach high point at 10 months, compared to 12)

61%

Phishing simulation success rates—the act of reporting a simulation and not skipping or failing it—in critical infrastructure begins lower but winds up 61% higher after 12 months than the global average.

5.3%

Failure rates – clicking on a malicious link in a simulated phishing email – are 5.3% in critical infrastructure, slightly above the 5.1% global average. Impressive, given the higher participation rate.

Failure rates

Critical infrastructure employees are unusually active and high-performing in threat reporting behavior.

65%

Miss rates—not participating with a phishing simulation—start higher in critical infrastructure but after 12 months are 65% lower than the global average.

11.4%

The most effective type of phishing attack – spoofed internal organizational communications – induces an 11.4% higher failure rate with critical infrastructure than the global average.

Departments

Sales departments in critical infrastructure have unusually low failure rates compared to all other industries.

Marketing and communications departments in critical infrastructure have the highest phishing simulation failure rates, similar to the global trend, but the failure rate is higher.

Cyber-risk concerns around critical infrastructure

Cyber threat landscape and the CISO

Data breaches have outsized costs and consequences in the critical infrastructure sector. North America felt the shock of fuel supply chain disruption with the Colonial Pipeline ransomware attack in 2021 [3]. And as cyberattacks on hospitals have doubled each year since 2016, according to JAMA [4], IBM has reported that the healthcare sector's $10.2 million cost-per-data-breach makes it the hardest-hit of all sectors for twelve years running in their Cost of a Data Breach Report [5].

The 2023 Verizon DBIR reported that phishing is the top mechanism of social engineering breaches [6]. While ransomware remains a tremendous problem, the incidence of BEC attacks – fraudulent messages from threat actors posing as a trusted person or authority figure – have long been the kingpin of cybercrime according to the FBI [7], and they doubled in data breach incidences in 2022.

The energy sector is one of the top targets for social engineering and phishing attacks across all industries. Energy & utility data weigh heavily within this report's representative critical infrastructure sectors.

Social Engineering incidents have increased from the previous year largely due to the use of Pretexting, which is commonly used in BEC, almost doubling since last year. Compounding the frequency of these attacks, the median amount stolen from these attacks has also increased over the last couple of years to $50,000... When responding to social engineering attacks (and the same could be said of most attacks), rapid detection and response is key."

– VERIZON DBIR 2023 [8]

Information security leaders operating within the critical infrastructure space are particularly keen to map and mitigate their human risk due to a confluence of factors:

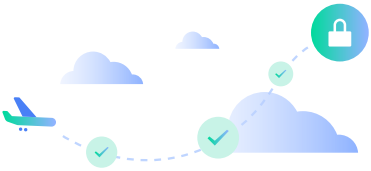
Shrinking security budgets and mounting attacks demand innovative strategic approaches.

Increasing regulatory pressure: Higher standards and increasing accountability.

Elevated target share from both profit-and-politically-motivated bad actors.

CEO and Board-level recognition of the CISO and cybersecurity as a business imperative.

New era of supply chain attacks.



Compliance

Tightening compliance standards for cybersecurity insurance and business partnerships.

Evolving threat landscape

AI and other advanced technologies are being adopted by increasingly sophisticated cybercrime-as-a-service models, state-sponsored actors, and criminal organizations.

People represent the largest cyberattack surface

In a time when they're being asked to reduce more risk with fewer resources, CISOs are seeking new ways to reduce risk at its greatest source.

In May of 2023, a joint Cybersecurity Advisory (CSA) was announced by the United States and international authorities [9] after Microsoft uncovered Volt Typhoon, a highly sophisticated and stealthy Chinese state-sponsored espionage campaign targeting US critical infrastructure for the purpose of disrupting.

> *"We face a complex threat environment, with state and non-state actors developing and executing novel campaigns to threaten our interests. At the same time, next-generation technologies are reaching maturity at an accelerating pace, creating new pathways for innovation while increasing digital interdependencies."*
>
> *— National Cybersecurity Strategy, March 2023* [10]

Phishing and critical infrastructure by the numbers

The number of attacks launched on critical infrastructure by nation-state actors doubled from **20% to 40%** of all threat activity, according to the 2022 Microsoft Digital Defense Report [11]. The 2023 Verizon DBIR broke down total social engineering breaches as 89% financially motivated and 11% for espionage [12].

In the White House's National Cybersecurity Strategy report, protecting critical infrastructure was spotlighted as the first of its five strategic pillars. The US Government Accountability Office highlighted the threat of targeted spear-phishing campaigns in software supply chain attacks in its most recent Cybersecurity High-Risk Series: Challenges in Protecting Cyber Critical Infrastructure [13].

Cybersecurity Ventures reports that cybercrime will cost global businesses **$8 trillion** in 2023 [14]. According to the Information Risk Insights Study performed by CISA and the Cyentia Institute, a typical cyber incident costs **$266,000**, but in the top 5% of loss events, that figure balloons to **$52 million**, and the largest weighed in at a whopping $12 billion [15]. The same report found that large organizations with over $100 billion in annual revenue—including many energy & utilities companies—are **32 times more likely** to have multiple security incidents in a year than smaller firms.

The FBI's IC3 report states that phishing was the number one type of cybercrime in 2022, and BEC was the most costly [16]. Indeed, be it to deploy a BEC or wire fraud attack, ransomware, or other forms

of malware, attackers overwhelmingly target people with phishing attacks to gain access to networks and data. 2022 Verizon Data Breach Incidence Report [17] and the World Economic Forum report that **82 % and 95 % of breaches contain the human element** and/or are due to human error, primarily related to phishing.

Phishing attacks are becoming increasingly targeted and sophisticated with new technologies like AI and large language models like ChatGPT, according to the White House [18]. IBM reports that the average cost of a data breach in the United States has climbed year over year to **$9.44** million, which is **$5.09** million more than the global average, and the energy sector incurred the fifth-highest cost per data breach at **$4.72 million** [19]. Meanwhile, the average annual cost of phishing more than tripled to **$14.8 million** between 2015 to 2021 [20], according to the Ponemon Institute's most recent Cost of Phishing study, which also reported that a good security training program could cut those losses in half.

People are your greatest security ~~risk~~ resource

While there's a fair amount of information on the costs and challenges associated with phishing attacks and human risk, there are comparatively fewer studies on solutions and human risk reduction. The Gatner Innovation Insight on Security Behavior and Culture Program Capabilities -report supports the growing trend towards security behavior change programs over security awareness training (SAT) tools [21]. A risk-based approach to security begins with visibility into your largest attack surface: your people. It ends with providing them the skills and tools to defend themselves, join forces with the security team, and secure the organization. People reinforce the processes and technology in an information security system.

Methodology: How behavior change programs work in critical infrastructure environments

Hoxhunt's security behavior change program is significantly different from traditional SAT tools. Understanding how Hoxhunt works helps to appreciate these findings.

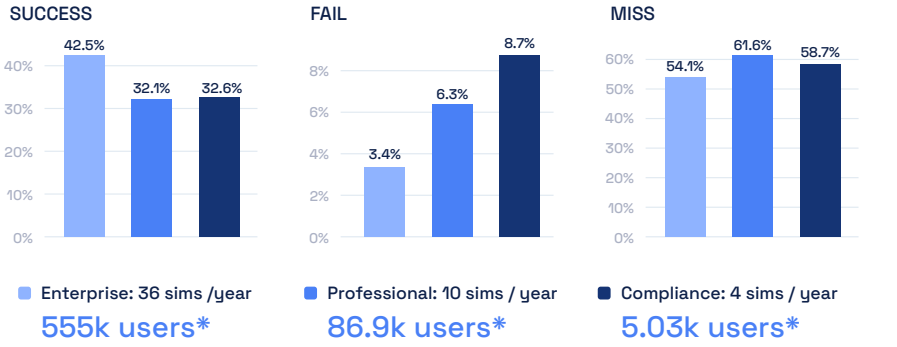
Hoxhunt results are based on organizational engagement rates that typically range from 38–60% and occasionally touch over 90%. That compares favorably with legacy SAT tools, which typically range between 5–20% according to benchmark studies with customers seeking to mature their human risk posture beyond what Gartner characterizes as the SAT model's limited capabilities [22].

> *Security awareness computer-based training services offer a stable set of core capabilities yet risky employee behavior persists. New, emerging capabilities apply behavioral science principles, data analytics and automation to help cybersecurity leaders reduce risk via measurable culture change.*
>
> *– Innovation Insight on Security Behavior and Culture Program Capabilities, Gartner, Nov. 16, 2022*

Engagement with Hoxhunt requires interacting with a phishing simulation to report it via a button integrated with the email client

or to click a simulated phishing link. Engagement with an SAT tool is less outcome-based and more opaque, as everything other than failing a phishing simulation is counted as a success.

More simulations improves skill and lowers failure rate



*User size samples

Analyzing 3 user cohorts defined by number of simulations received per year (36, 10, or 4), we found a direct correlation between the number of simulations and user failure rate. Practice makes perfect.

Moreover, real threat detection activity is tracked with Hoxhunt, as users are rewarded with AI-enabled instant feedback when they report a suspicious email. **Real threat detection rates climb to over 60% with active Hoxhunt users.** In SAT tools, real threat detection activity is usually not calculated or negligible.

High behavior-based engagement with phishing emails in and outside training produces more data points. This better reveals true human risk and reduces unknown and assumed risks. With

Hoxhunt, dozens of phishing simulations are automatically sent to users every year, which automatically adapt to individual users' skill levels and backgrounds via an AI-generated adaptive learning model on a gamified learning journey. This compares favorably to the four cookie-cutter simulations sent yearly in traditional SAT programs.

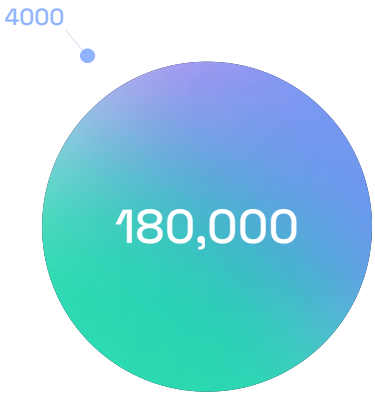
These factors yield exponentially more data points. Leveraging the behavioral science of nudge techniques via microtrainings, Hoxhunt rewards action on a phishing simulation's success (threat reporting) and failure (link clicking). Micro-learning moments are triggered after every interaction.

→ Rewarding success and teaching on failure mark a crucial departure from the failure-based model of traditional SAT tools, which give a fundamentally limited picture of organizational risk and fail to measurably reduce human risk, as the Verizon DBIR and Gartner have concluded.

Exponentially fewer data points are available with an unengaged employee population. In a hypothetical 10,000-person company, an SAT tool that produces a 10% engagement rate with 4 simulations per year, compared to a behavior change program with a 50% engagement rate on 36 simulations per year, breaks down to:

SAT:
4000 data points, confined to a small cohort

Behavior change:
180,000 data points, representing a statistically significant cohort



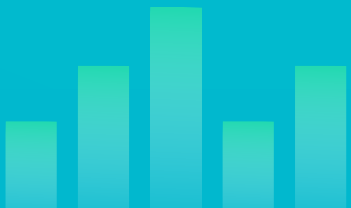
* A note on nudges vs. time as an X-axis measurement: Hoxhunt automatically sends one individualized phishing simulation every 10 days, approximately. The core principles of applied behavioral science [23], such as the work on persuasive technology [24] by Stanford's B.J. Fogg, stress practice, and prompts for behavior change.

* A note on meaningful metrics and the resilience ratio [25]: the success rate is more significant than the engagement rate or failure rate because threat reporting success measures and improves the behavior you're trying to change. That's why we recommend calculating the resilience ratio by dividing the success rate—not the engagement rate—by the failure rate. There's a difference. Whereas reporting a simulated threat is a clear outcome, engagement can be mysterious or inaccurate from one platform to the next.

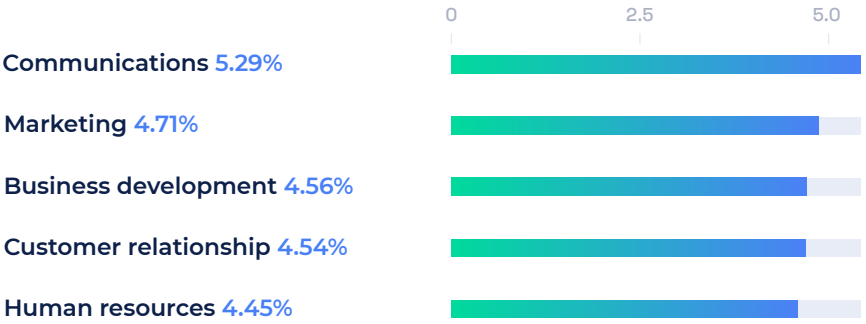
REPORTED

Top threats to watch out for in critical infrastructure: by department

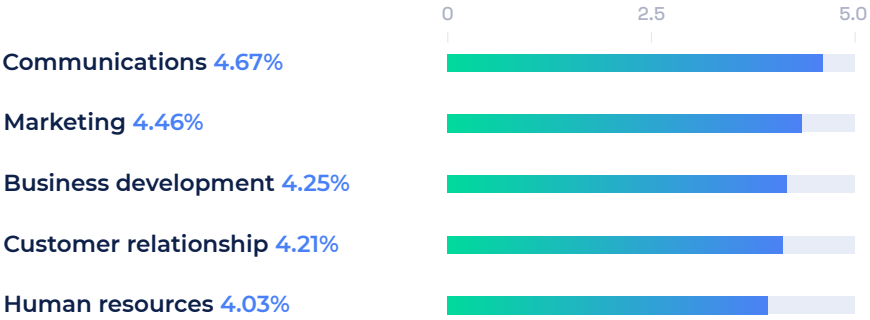
The departments within the critical infrastructure industry that are most likely to fall for phishing attacks are Communication, Marketing, and Business Development. The most resilient departments are Finance, Sales, and Legal. These results track with global averages except for the high performance of Sales, whose performance in critical infrastructure is better than the global average.



Highest fail rate: Job functions – Critical Infrastucture

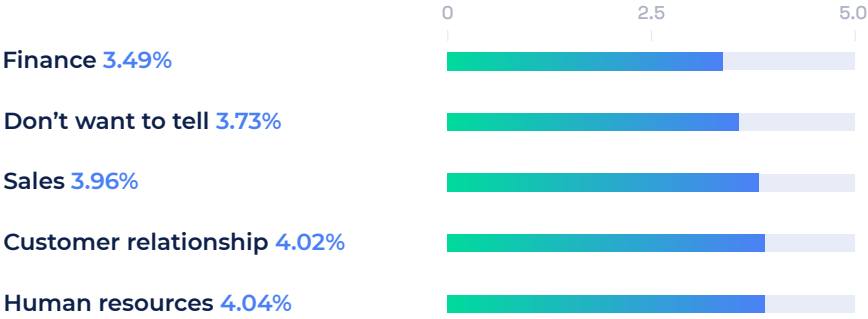


Highest fail rate: Job functions – Global Average

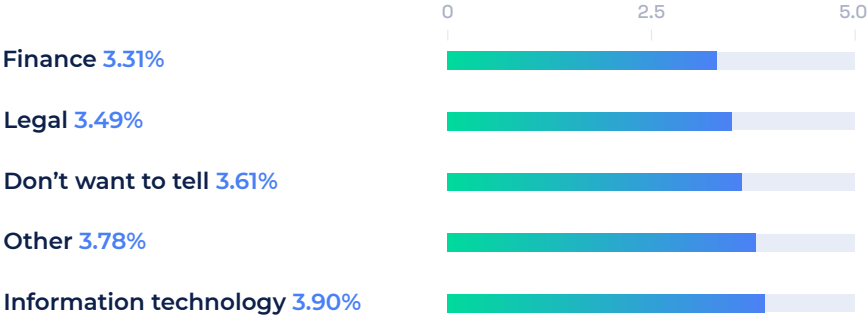


→ The departments within the critical infrastructure industry that are most likely to fall for phishing attacks are Communication, Marketing, and Business Development.

Lowest fail rate: Job functions – Critical Infrastucture



Lowest fail rate: Job functions – Global Average



→ These results track with global averages except for the high performance of Sales, whose performance in critical infrastructure is better than the global average.

Sales departments in critical infrastructure have unusually low failure rates compared to all other industries.

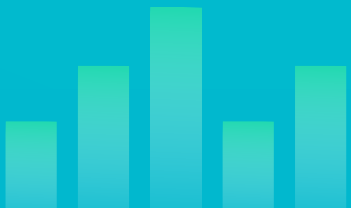
Marketing and communications departments in critical infrastructure have the highest phishing simulation failure rates, similar to the global trend, but the failure rate is higher.

REPORTED

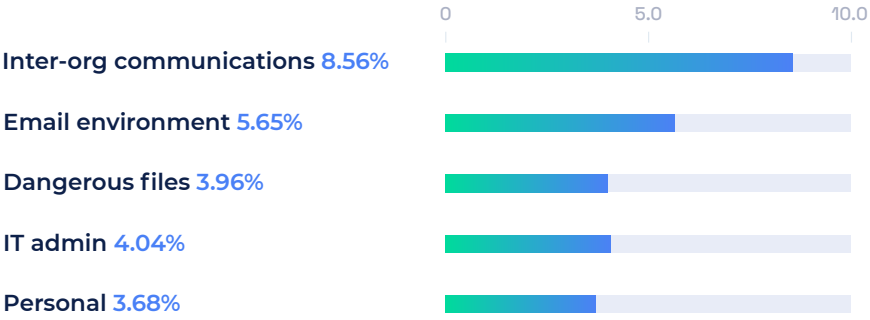
Most dangerous types of phishing attacks on critical infrastructure

Critical infrastructure employees will most likely fall for a phishing attack spoofing internal organization communications. This type of attack could be, for example, a fraudulent message from HR or IT promising a reward if action is taken or threatening a consequence if action isn't taken.

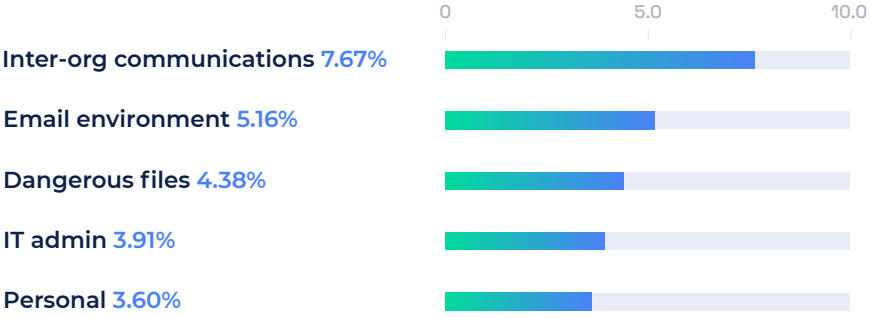
These results are precisely aligned with the global average, albeit with a higher failure rate on internal org communications.



Highest fail rate: Themes – Critical Infrastucture



Highest fail rate: Themes – Global Average



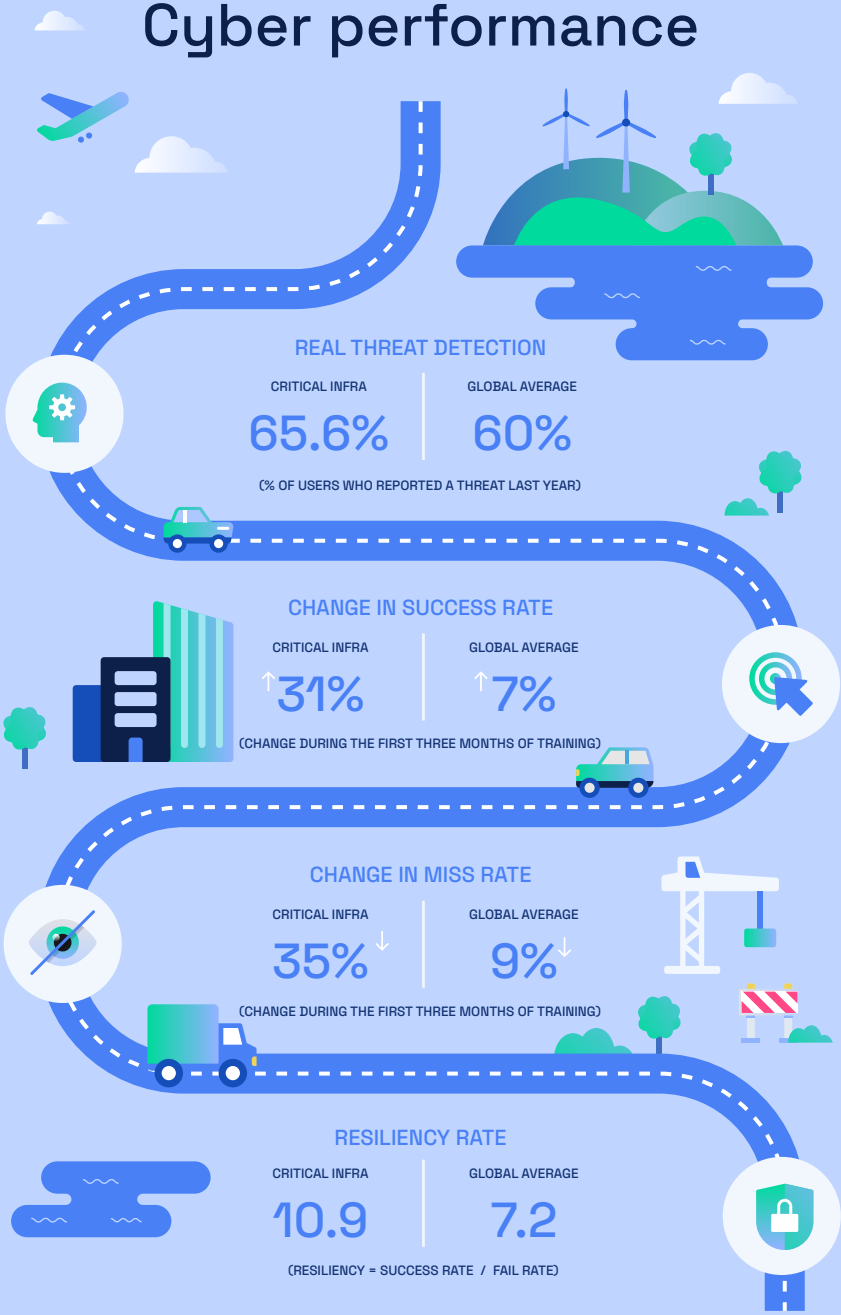
→ Critical infrastructure employees will most likely fall for a phishing attack spoofing internal organization communications.

Phishing simulation results after a behavior change program

Success means reporting a simulated phishing attack. Improvement in success rate reflects the effectiveness of a behavior change program. Simultaneously, a decline in miss rate, or the rate at which people don't interact with a phishing simulation, gives visibility into the organization's actual (rather than assumed) human risk posture. The miss rate is a significant predictor of real threat detection behavior, according to previous Hoxhunt research [26]. High miss rates correlate to low real threat detection rates, but those actively engaged in training also report more real threats.

→ Failure rate must be considered within the context of success and miss rates. Standing alone, it's a poor indicator of human risk or cybersecurity performance and progress.

Cyber performance



→ Critical infrastructure employees are comparatively more engaged in training, as their reporting and miss rates indicate. They show better overall threat-reporting behavior than the global average.

Training changes behavior more effectively in critical infrastructure organizations than the global average:

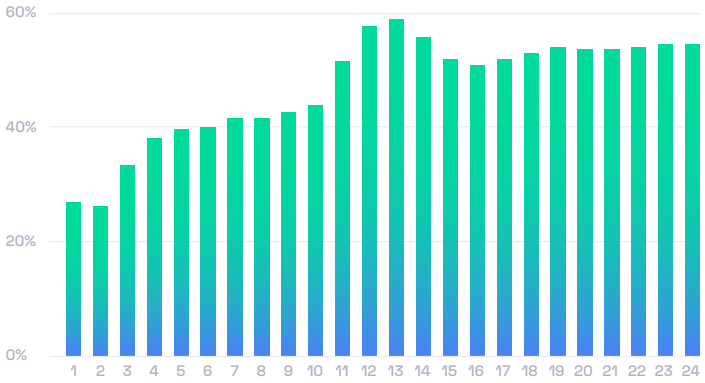
- Phishing simulation success rates—the act of reporting a simulation —in critical infrastructure begins lower but winds up **61% higher** after 12 simulations (about 3 months) than the global average.

- Miss rates—not participating with a phishing simulation—start higher in critical infrastructure but, after 12 simulations, are **61% lower** than the global average.

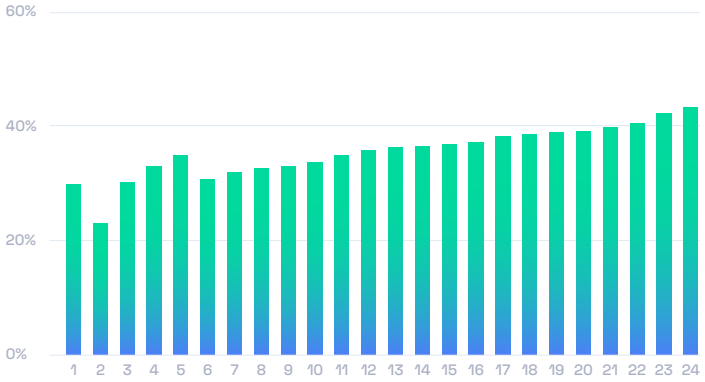
- Success rates improved **from 27% to 58%** compared to 29% to 36% against the global average in the first 12 simulations, or 4 months, of using Hoxhunt.

Success

Industry success rate progression by simulation
Critical Infrastucture

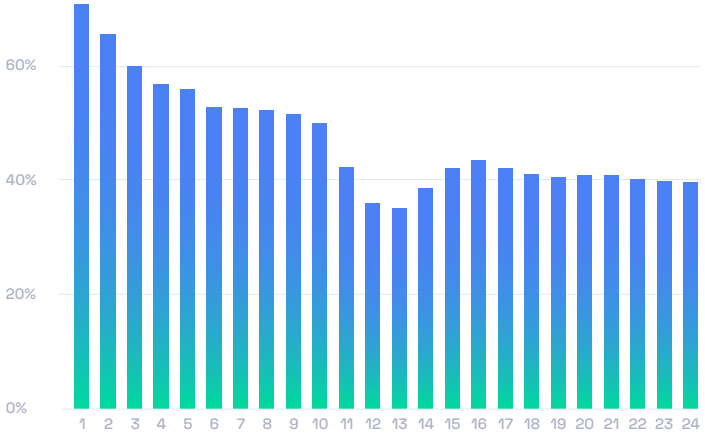


Industry success rate progression by simulation
Global Average

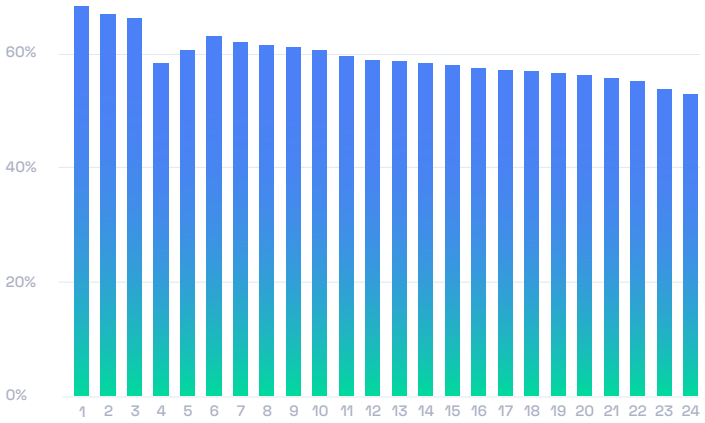


Miss rate

Industry miss rate progression by simulation
Critical Infrastucture



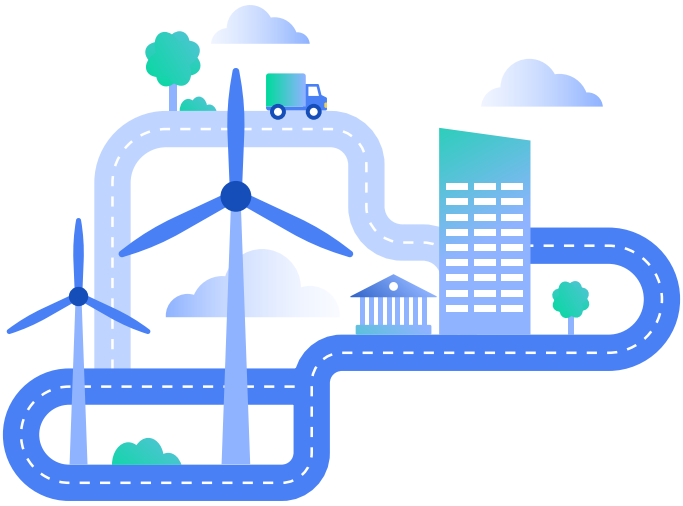
Industry miss rate progression by simulation
Global Average



Key findings

- **Resilience ratio (success rate/failure rate) is 51% higher** than the global industry average: 10.9 for critical infrastructure vs. 7.2 for the global average.

- **Resilience velocity is 20% higher:** Users reach the point of diminishing returns in terms of threat reporting after 10 simulations, or roughly 100 days, in the Hoxhunt program, two simulations, and approximately 20 days faster than the global average.

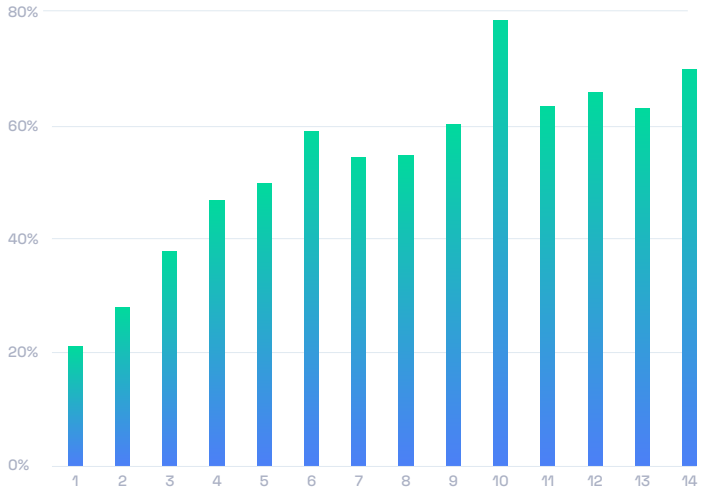


Real threat detection

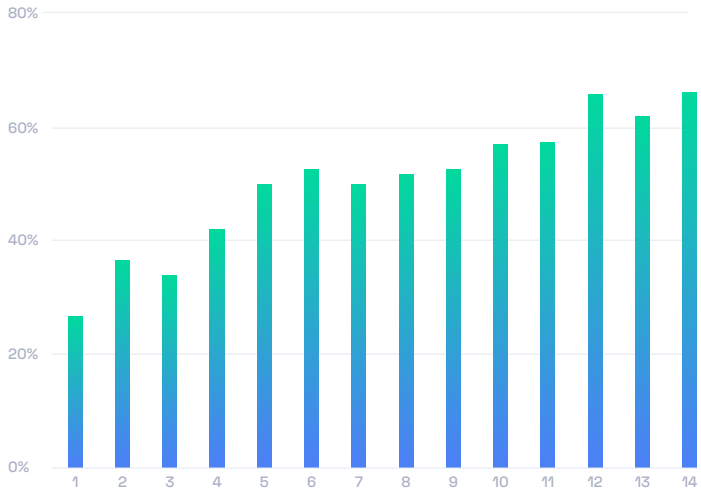
The ideal outcome of a phishing attack is a threat report. A phishing report removes the threat from the system, alerts the security team, and accelerates SOC response to neutralize the incident before it spreads. People are the SOC team's lighthouse for catching the sophisticated threats that bypass email filters.

→ **Resilience velocity: the speed at which the organization reaches its highest level of actual threat detection behavior. Critical infrastructure has a 20% higher resilience velocity, reaching the point of diminishing returns in 10 months compared to 12 months on the global average.**

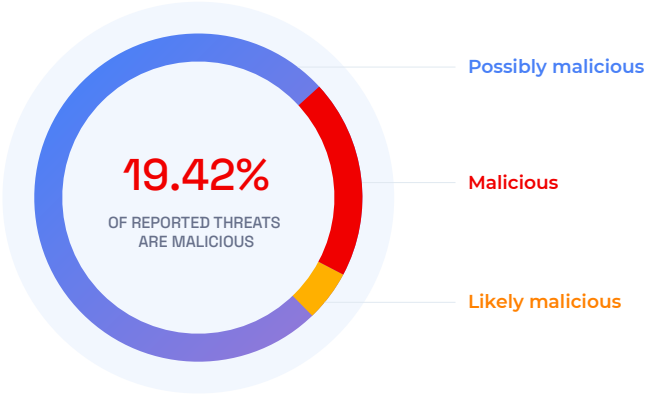
Reporting users by month – Critical Infrastucture



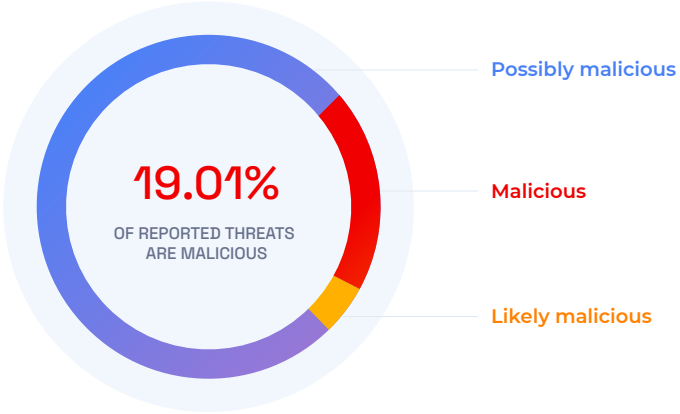
Reporting users by month – Global Average



Reported malicious emails – Critical Infrastucture



Reported malicious emails – Global Average



→ Threat detection accuracy indicates skill level.

The proportion of threat reports that detect malicious emails reflects skill. Threat reporting accuracy shows how well a person can recognize and report a phishing attack.

Key findings

- **Threat reporting doesn't stop at training.**
- **A direct relationship exists** between participation in a security behavior change program and real threat detection activity and accuracy.
- **20%** higher resilience velocity. Critical infrastructure employees reach a point of diminishing returns in 10 months compared to 12.
- Critical infrastructure employees report malicious threats with **nearly the same accuracy** as the global average.
- The relationship between training and real threat detection gives important evidence that **security behavior change measurably reduces risk**.

Discussion

Resilience doesn't end in the classroom. Due to Hoxhunt training, over 60% of 1.6 million program participants actively recognized and reported real threats in the previous year. Each threat report bolstered organizational security and reduced the risk of a breach. Hard data is scant, but threat detection rates typically run between negligible to 5% in a company without a behavior change program, according to qualitative surveys of Hoxhunt admins. This link between behavior change training and real threat detection has never been reported— its importance can't be overstated.

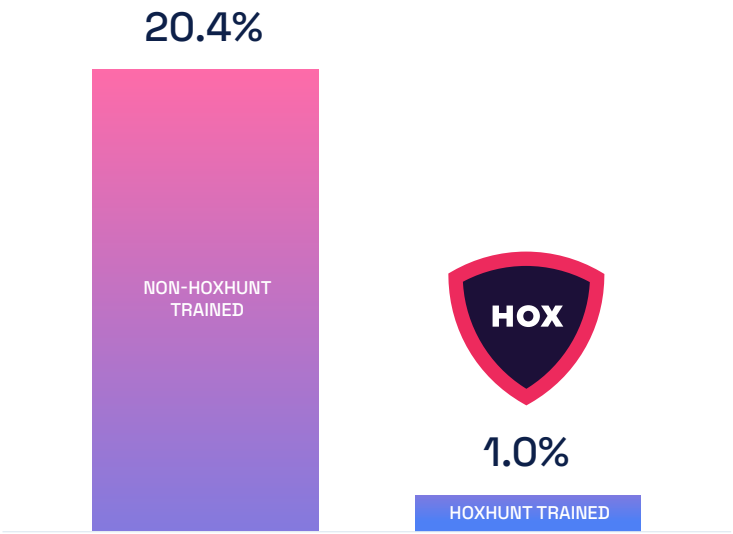
This exponential increase in real threat detection activity presents the SOC team with an enviable problem: an abundance of threat reports.

→ Human risk is defined by behavior. Cyber performance in the energy and utilities space tends to show exceptionally well, as can be demonstrated by numerous case studies.

CASE STUDY: elisa

→ Human risk management in energy and utilities is of special importance in Finland, which has endured increased cyberattacks since its application and acceptance to NATO. One bad click could lead to a massive power outage.

In an independent benchmark study conducted by Elisa, Finland's largest telecom, the phishing simulation performance of 2,000 employees from 11 companies using SAT tools was compared against 1,000 Hoxhunt-trained employees from Finland's largest power grid, FinGrid. The utility company employees' phishing simulation failure rates were 20 times lower than those of the SAT-trained employees.



CASE STUDY: aes

→ Energy companies have experienced among the greatest organizational risk reductions that we at Hoxhunt have seen. Fortune 500 energy company AES recently reported an astonishing 2,533% increase in their resilience ratio after switching from their legacy SAT model to a security behavior change program.

Hoxhunt vs. 3 major security awareness tools

526%

increase in reporting rate
from 11.5% to 60.5%

79%

decrease in failure rate
from 7.6% to 1.6%

58%

decrease in miss rate
from 80.9% to 34%

2533%

increase in resilience ratio
from 1.5 to 38

Fortune 500 Telecom
Benchmark Case Study

→ In a unique benchmark study, a Fortune 500 telecom company emptied out their phishing jail's 1000 worst repeat offenders, trained them with Hoxhunt for three months, and compared their performance against 1000 of their SAT-tool-high-performing peers. Recording a 102% higher resilience ratio than their peers, the formerly-low-performers showed that even the biggest security risks could be reformed into security assets.

Conclusion

Security behavior change works – when it's done right. Training that's designed to measure and improve the desired behavior changes that behavior and demonstrably reduces the risk of a phishing breach.

Awareness and compliance signify only the beginning of a human risk management journey. Behavior change and measurable risk reduction represent that journey's end.

That journey contains many steps, or nudges. No 1-4 testing package will equate to a leap from zero awareness to resilience. The below graph demonstrates the power of practice in terms of behavior change.

The cybersecurity community is at a crossroads of human risk. Mounting business and geopolitical pressures require improvements in risk posture to be measurably achieved and communicated to boards, business partners, and regulatory bodies. Resilience is a business driver. Human risk posture is a competitive advantage.

→ These human risk results presented in this report are robust because they're derived from a security behavior change program, not an SAT tool. We invite you to read Gartner's report on the rise of what they call Security Behavior and Culture Programs.

Training changes behavior more effectively in critical infrastructure organizations than the global average:

- By 2030, **80%** of enterprises will have a formally defined and staffed human risk management program, **up from 20%** in 2022.

- By 2030, all widely adopted cybersecurity control frameworks will focus on **measurable behavior change rather than compliance-based training** as the critical measure of efficacy for human risk management.[27]

Most cybersecurity leaders report lofty aspirations for their security awareness programs yet underinvest in this space because legacy solutions don't meet current CISO needs. Under half of cybersecurity functions consistently measure employee behavior, and almost 80% have less than one FTE dedicated to security awareness (Figure 1). Cybersecurity leaders are hesitant to invest more resources and effort until solutions reliably deliver better risk management results.

– INNOVATION INSIGHT ON SECURITY BEHAVIOR AND CULTURE PROGRAM CAPABILITIES, GARTNER, NOV. 16, 2022

References

1. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

2. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

3. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

4. https://jamanetwork.com/journals/jama-health-forum/fullarticle/2799961

5. https://www.ibm.com/reports/data-breach

6. https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/social-engineering/

7. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

8. https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/social-engineering/

9. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a

10. National Cybersecurity Strategy, March 2023

11. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

12. https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/social-engineering/

13. https://www.gao.gov/products/gao-23-106441

14. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

15. https://www.cyentia.com/iris/

16. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

17. https://www.verizon.com/business/resources/reports/dbir/

18. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

19. https://www.ibm.com/reports/data-breach

20. https://ponemonsullivanreport.com/2021/08/#:~:text=The%20cost%20of%20phishing%20more,to%20%2414.8%20million%20in%202021

21. https://www.hoxhunt.com/blog/gartner-names-hoxhunt-a-security-behavior-and-culture-change-program-representative-provider

22. https://www.hoxhunt.com/blog/gartner-names-hoxhunt-a-security-behavior-and-culture-change-program-representative-provider

23. https://www.hoxhunt.com/case-studies/docusign-and-the-psychology-of-behavior-change-for-cybersecurity-training-with-hoxhunt

24. https://www.sciencedirect.com/book/9781558606432/persuasive-technology

25. https://www.hoxhunt.com/blog/security-behavior-change-to-measure-true-risk-and-manage-human-risk

26. https://www.hoxhunt.com/behavioral-cybersecurity-ebook

27. Innovation Insight on Security Behavior and Culture Program Capabilities, Gartner, Nov. 16, 2022

THE HUMAN RISK REPORT SERIES · 2023