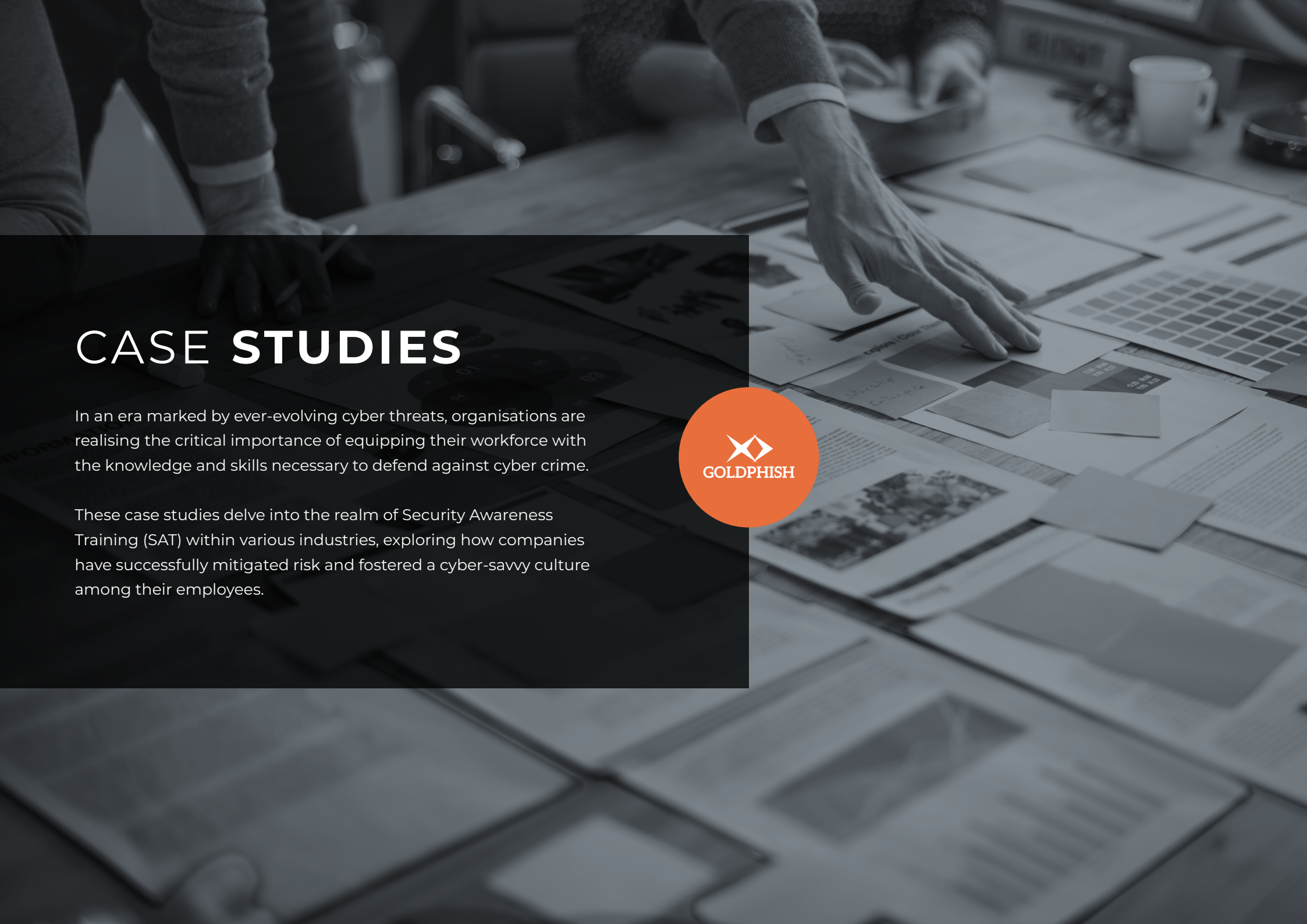


CASE **STUDIES**

In an era marked by ever-evolving cyber threats, organisations are realising the critical importance of equipping their workforce with the knowledge and skills necessary to defend against cyber crime.

These case studies delve into the realm of Security Awareness Training (SAT) within various industries, exploring how companies have successfully mitigated risk and fostered a cyber-savvy culture among their employees.

GOLDPHISH

GOLDPHISH

CASE STUDY

Industry: ***Finance***
Organisation Size: ***70***
Country: ***USA***

OVERVIEW

A boutique accounting firm struggled with cyber security challenges, experiencing phishing attacks and lacking insurance due to no Security Awareness Training (SAT).

To meet IRS and regulatory requirements and build a cyber-savvy workforce, they sought an interactive SAT solution. They wanted a user-friendly platform offering engaging training content accessible at employees' convenience, unlike traditional security seminars.

THE PROBLEM

Due to a phishing attack, the client, an accounting firm handling sensitive data, became uninsurable due to insufficient cyber security knowledge. They initially engaged an MSP for basic hourly training to meet IRS regulations but found it ineffective. Recognising the importance of tailored and on-demand training, the client sought a solution that would enable them to conduct training and simulated phishing campaigns conveniently, ensuring the security of their information and becoming insurable.

THE SOLUTION

To effectively tackle these challenges, the client partnered with GoldPhish to establish a robust security awareness program and foster a secure culture within their organisation. The primary objective was to align with IRS requirements while elevating cyber security awareness throughout the firm. Recognising the critical need to address their vulnerability, the client seamlessly integrated GoldPhish and promptly initiated regular monthly training and simulated phishing campaigns.

These proactive measures aimed to equip employees with essential knowledge and skills to identify and mitigate cyber threats effectively, ensuring the organisation's compliance and resilience in the face of evolving cyber risks.

> We have not fallen victim to any subsequent phishing attempts since implementing GoldPhish's solution.

THE RESULT

As a result of their partnership with GoldPhish, the client witnessed a notable surge in employees reporting phishing attempts, effectively strengthening their overall security posture. This proactive approach ensured the organisation's continued insurability, reinforcing their commitment to robust cyber security practices.

Moreover, since the implementation of GoldPhish's solution, the client has remained resilient, successfully averting any subsequent phishing attacks. The combination of comprehensive training and simulated phishing campaigns offered by GoldPhish empowered employees to recognise and respond to potential threats, significantly reducing the organisation's vulnerability to phishing attacks and enhancing their overall cyber security resilience.

GOLDPHISH

CASE STUDY

Industry: ***Insurance***
Organisation Size: ***20+***
Country: ***USA***

OVERVIEW

A major jewellery insurance firm in the United States of America (USA) initially engaged GoldPhish to simply meet audit requirements.

However, after successfully complying with regulations and conducting several simulated phishing campaigns and training campaigns, using the GoldPhish solution, they recognised the significant impact a comprehensive Security Awareness Training (SAT) solution has in reinforcing their security measures.

THE PROBLEM

The client, a fast growing company with over 2,500 clients across the USA, faced two major challenges. Firstly, they needed to protect their organisational information and ensure the security of their clients' sensitive data. Secondly, they had to address the low employee engagement and limited effectiveness of their existing SAT solution. This critical state left them vulnerable to cyber attacks and ineligible for cyber insurance due to their poor cyber security posture and failure to meet audit requirements.

THE SOLUTION

In response to their low employee engagement and lack of company buy-in to their existing SAT efforts, they utilised GoldPhish to develop a 12-month cyber security plan to help meet their requirements and increase employee engagement. Recognising the organisation's vulnerability, the client was successfully onboarded and immediately implemented monthly training and simulated phishing campaigns.

They had experienced numerous phishing attempts. This accompanied by the inexperience of their employees, resulted in the organisation being high-risk . After partnering with GoldPhish, they observed an increase in the reporting of real phishing attempts and began to achieve consistently lower scores in their monthly simulated phishing campaigns.

> GoldPhish has helped make security awareness training readily and easily available to all employees

THE RESULT

By adopting GoldPhish's training and simulated phishing solution as their efforts to reduce human element to their cyber risk, as well as accessing and making use of the GoldPhish value-added communications content on a monthly basis, they ensured training to their employees that is:

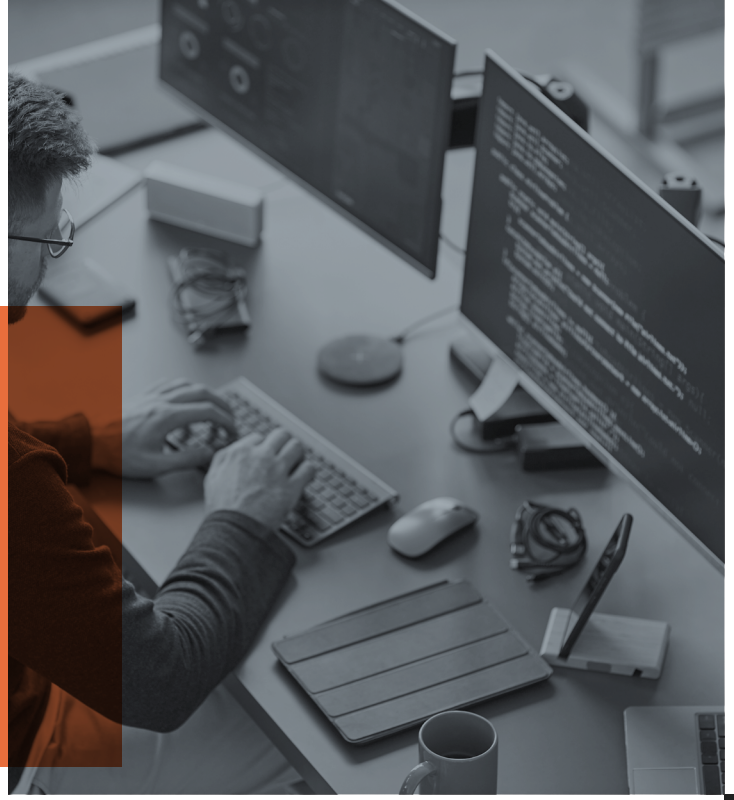
- **consistent**
- **relevant**
- **relatable**

This partnership with GoldPhish has fostered a more cyber-secure culture within the organisation and has helped make SAT readily and easily available to all employees. As a result, they have empowered their workforce to play an active role in safeguarding online information, both at work and at home.

GOLDPHISH

CASE STUDY

Industry: ***IT & Services***
Organisation Size: ***30+***
Country: ***SA***



OVERVIEW

A South African IT company engaged with GoldPhish to enhance cyber security awareness and comply with regulations. Seeking ISO27001 certification, the client, dealing with sensitive data, implemented simulated phishing and training campaigns.

GoldPhish's comprehensive Security Awareness Training (SAT) solution reinforced security measures and met ISO certification requirements, making a significant impact on their overall cyber security posture.

THE PROBLEM

The client, a leading player in consumer intelligence, partners with 80+ major African banks, insurers, retailers, and healthcare organisations. They had two key challenges: Safeguarding organisational data and securing clients' sensitive information, and mitigating increased cyber security risks with remote work.

Prior to engaging GoldPhish, employees lacked SAT, making them vulnerable to cyber attacks and ineligible for insurance due to weak cyber security.

THE SOLUTION

Through the partnership with GoldPhish, the client gained access to a range of customised SAT modules and simulated phishing campaigns. These training initiatives were tailored to address the specific needs of the organisation and its employees. The comprehensive 12-month cyber security plan incorporated regular assessments, progress tracking, and continuous improvement strategies.

By actively engaging employees in ongoing security training and simulated phishing exercises, the organisation witnessed a significant improvement in their cyber security posture. This proactive approach not only enhanced their eligibility for cyber insurance but also instilled a culture of cyber security consciousness across the organisation.

> GoldPhish has increased employees' cyber security awareness, and has resulted in an increase of 40% of reported phishing attempts.

THE RESULT

They **increased their employees' reporting of phishing attempts from 0% to 40%.** Moreover, they successfully met regulatory standards and requirements, obtaining their ISO certification.

This partnership with GoldPhish fostered a more cyber-secure culture within the organisation and facilitated the easy accessibility of SAT for all employees. As a result, they empowered their workforce to actively contribute to safeguarding online information, both within the workplace and at home.

GOLDPHISH

CASE STUDY

Industry: ***Communications***
Organisation Size: ***500+***
Country: ***USA***

OVERVIEW

A leading corporate communications agency faced cyber security hurdles, including low employee engagement and uninsurability due to the absence of Security Awareness Training (SAT).

They acknowledged the urgency of implementing stronger cyber security practices, given their work with global brands. The organisation's vulnerability and uninsurable status highlighted the need for immediate action.

THE PROBLEM

The lack of cyber security knowledge and unsuccessful previous attempts at SAT left them vulnerable. Wanting to include cyber insurance in their coverage, they were redirected to GoldPhish. Before, they had a basic cyber security policy with employee acknowledgment but lacked further active measures. The lack thereof left them vulnerable to cyber attacks and having a poor overall cyber security posture.

THE SOLUTION

To tackle these challenges, the client along with their insurer enlisted GoldPhish for comprehensive SAT and simulated phishing. The objective was to meet new cyber insurance standards and enhance awareness of cyber security throughout the organisation. Aware of their vulnerability, they swiftly integrated GoldPhish and implemented monthly training and simulated phishing campaigns.

Accompanied by GoldPhish on their journey to becoming a more cyber-savvy workforce, they managed to mitigate future risks and become a low-risk organisation. A security plan was put in place to help the organisation increase their employee engagement and become insurable due to the active practice of SAT within the organisation.

> The shorter training campaigns have allowed the employees to complete training on a monthly basis and this has strengthened our overall cyber security posture.

THE RESULT

They achieved significant positive outcomes. Notably, employee engagement with the SAT initiatives increased, with employees actively reporting phishing attempts. The implementation of shorter, monthly training campaigns facilitated regular skill-building and strengthened their overall cyber security posture. The proactive approach, coupled with evidence, provided through executive progress and performance reports, resulted in the successful maintenance of their insurability.

Through their partnership with GoldPhish, they met the new cyber insurance standards but also developed a more cyber-aware workforce. They significantly reduced their vulnerability to cyber attacks, thereby safeguarding their reputation and ensuring continued business operations.