Cyberfort
Expert-led. Security Driven.

Case Study

Discover how a market leading global insurance company used Cyberfort Broad Security Review, Purple Teaming and InfoSec Awareness services to improve their cyber resilience in a highly regulated environment

Industry:
Insurance

Location:
Worldwide

01304 814800 | cyberfortgroup.com | info@cyberfortgroup.com

Introduction

In this case study we cover the work Cyberfort has undertaken for a global insurer established for over a hundred years with thousands of staff serving clients across commercial, manufacturing, and service industries. They have a portfolio of innovative, insurance solutions designed to address the full spectrum of business risk and manage premium volumes exceeding 10 billion euros annually.

As the business has grown it was recognised the company was facing an increasingly sophisticated threat landscape, changing regulatory requirements across multiple jurisdictions, and growing awareness that human error potentially represented their single largest attack risk.

To keep pace with the evolving threat landscape, changing regulatory environments in several countries they were operating in and ensure they were resilient against attack, they partnered with Cyberfort to deliver a broad security review spanning people, processes, and technology, undertook a Purple Teaming exercise and a structured staff information security awareness campaign.

The broad security review encompassing governance frameworks, identity and access management, data classification, vendor risk management, and incident response readiness provided the strategic foundation. Purple Teaming tested where potential gaps may exist and how they would respond to an attack. InfoSec training for key teams within the company was also put in place to ensure staff in a variety of different job roles understood what the cyber security risks were and how to make sure they were taking the right action should they be targeted by an attacker. This case study examines the insurers approach, the rationale for engaging external specialist expertise, and the measurable outcomes achieved from the work undertaken by Cyberfort.

Cyberfort
Expert-led Security Driven

Understanding the digital environment and security posture

The insurer operates a global technology estate spanning underwriting platforms, policy administration systems, and distributed workforce environments across the world. With employees regularly accessing core business systems from outside the corporate perimeter, and a requirement to maintain third-party integrations with brokers, reinsurers, loss adjusters, and regulatory bodies having the right security systems, controls and processes in place and ensuring they were regularly tested, benchmarked and risks were fully understood would be crucial to business success.

The insurance sector is highly competitive and has several key regulations in relation to cyber security that must be adhered to. Previously the insurer had undertaken security reviews internally within each country business unit. As the business evolved, they recognised they needed an independent baseline assessment of the organisation's true risk exposure across people, processes, and technology platforms. A holistic security review, Purple Teaming exercise and InfoSec training programme for key members of staff would enable them to identify where actual risk existed, remediation plans could be created and gaps in staff knowledge in relation to cyber security could be addressed.

The evolving threat environment
Over several years, the insurers internal security team had identified a series of compounding risks.

These included:

Increased attacks on the financial services sector
With it estimated by industry reports that there has been a 200% increase in attacks targeting the financial services sector since 2023, and the cost of a cyber-crime incident 40% higher than other industry sectors, it was clear insurers were being targeted not only for financial gain but for the strategic value of the client data they hold. Many of the attacks on insurers over the past 3 years have centred around phishing and ransomware attempts directed at underwriters and claims handlers, the employees with the greatest access to sensitive client data and financial transactions.

Absence of an independent Broad Security Review
Although security reviews by the insurer had been taking place by individual country units, it was recognised, they may not be fully aware of all the risks that could potentially exist within their IT environment. To mitigate risks, they may not know about the insurer needed a documented baseline of its security maturity across the full control framework including governance, risk management, asset classification, identity and access management, vendor risk, data protection, business continuity, and incident response readiness. An independent holistic view would give a unified view of overall posture against industry benchmarks and the latest threat intelligence data a specialist MSSP like Cyberfort knows and understands in detail.

Needing further understanding of security gaps across different job roles
Due to the heightened risk of cyber security attacks targeting key staff members, they recognised security awareness training that was compliance-driven and focused on the most common attacks would be crucial both today and in the future. This would help them to remain secure and minimise the risks of human error.

Regulatory pressure and client expectations
As mentioned earlier the insurer had multiple overlapping regulatory regimes. These included DORA, and the FCA's Operational Resilience framework in the UK. The insurers commercial and manufacturing clients also increasingly required vendors, including insurers, to demonstrate robust cyber security posture as a condition of contract renewal.

01304 814800 | cyberfortgroup.com
info@cyberfortgroup.com

Cyberfort
Expert-led Security Driven.

Engaging with Cyberfort to improve Cyber Resilience

Following a market assessment the insurer appointed Cyberfort as a cyber security partner. They recognised Cyberfort had deep experience in the financial services and insurance sector. By engaging with Cyberfort for a Broad Security Review and InfoSec training they would have:

Access to specialist expertise

Cyberfort has a team of certified security professionals, security review consultants, threat intelligence analysts, and behavioural security specialists that would have taken the insurer several months to recruit and develop internally.

Operational independence

External specialists bring genuine objectivity, an internal team reviewing or testing systems they have helped design cannot replicate the independent, adversarial perspective of an experienced third party.

Speed to value

Cyberfort was able to mobilise a dedicated team and commence the broad security review within a few weeks of contract signature.

Cost efficiency and scalability

The Cyberfort model would allow the insurer to have enterprise-grade capabilities on a managed service basis, with the ability to access resources on demand during critical periods without permanent headcount commitments.

5 | Case Study | Insurance

Broad Security Review – Uncovering hidden risks and developing a clear action plan

Recognising that technical testing and behavioural training in the absence of a baseline understanding of overall security posture would risk misallocating remediation effort, Cyberfort commenced the engagement with a Broad Security Review. This assessment examined the insurers security maturity across control domains and benchmarked against a variety of cyber security frameworks. The Broad Security Review which was undertaken included:

Governance and risk management

Evaluation of the security governance structure, Board-level reporting, risk appetite statements, and the alignment of security investment to business risk priorities. The review would help to identify any gaps in the companies Information Security Management System (ISMS) and enable the development of board-approved cyber risk tolerance thresholds.

Asset and data management

Inventory assessment of hardware, software, and data assets. The review would identify where systems were running end-of-life, and any data classification gaps.

Vendor and supply chain risk

Assessment of third-party risk management processes across the insurer's ecosystem of technology and service suppliers.

Identity and access management

Review of user provisioning, privileged access governance, and third-party access controls. Excessive standing privileges could be identified and where multi-factor authentication was absent on remote access pathways.

Incident response and business continuity

Review of detection, response, and recovery capabilities.

The Broad Security Review produced a prioritised risk register and a security maturity roadmap, which showed risks vs urgency and business impact. By undertaking the Broad Security Review first, it would ensure that awareness training would address the behavioural gaps most directly linked to identified control weaknesses.

Cyberfort
Expert-led. Security Driven.

Purple Teaming - Bridging Offensive and Defensive Security

As part of the engagement, the insurer and Cyberfort introduced a structured purple teaming capability. The approach was collaborative with the aim of uniting the offensive expertise of red team attackers with the defensive intelligence of blue team defenders in a single, coordinated exercise.

The Broad Security Review had identified the gaps; purple teaming now answered the defining question: could the insurer see an attack happening, and could it respond effectively before any real business impact occurred?

The purple teaming exercises were structured around the insurers most critical threat scenarios, derived directly from the threat intelligence gathered during Cyberfort's initial engagement and mapped to an industry leading attack framework. Scenarios were selected to reflect the actual tactics, techniques, and procedures of threat actors known to target the insurance and financial services sector.

In each exercise, the red team executed a defined attack chain while the blue team comprising of the insurers internal SOC analysts working alongside Cyberfort threat detection specialists attempted to identify, alert, and contain each stage. Crucially, where the blue team failed to detect an action, the exercise paused, the technique was examined together, detection logic was written or corrected, and the attack was replayed to confirm the fix worked. This feedback-driven loop compressed what would otherwise be months of post-incident learning into focused, structured sessions, producing immediate, measurable improvements to the insurers SIEM rules, endpoint detection coverage, and analyst response playbooks.

For the insurer's security leadership, the exercises produced something that neither vulnerability reports nor compliance audits had previously delivered, empirical evidence of the organisation's true defensive capability under realistic attack conditions. For a global insurer whose clients expect the highest standards of security, the ability to demonstrate a quantifiably improving defensive capability validated by an independent MSSP has become a tangible competitive asset and a powerful component of their ongoing regulatory engagement narrative.

InfoSec Awareness Programme – Training staff to be aware and take action

Cyberfort designed a role specific InfoSec awareness programme that moved deliberately away from compliance checkbox training toward measurable behavioural change. The programme comprised of:

Baseline assessment

Simulated phishing campaigns and security knowledge assessments established a detailed picture of risk by department, seniority, and geography.

Targeted learning pathways

Content was segmented by role - underwriters, claims handlers, finance, IT, and senior leadership each received tailored modules addressing the specific threats and decision points relevant to their work.

Leadership engagement

A dedicated executive programme addressed social engineering risks specific to senior leaders, including CEO fraud, business email compromise, and regulatory impersonation scams.

The outcome from this exercise has shown that key staff members and the teams they operate in are now more confident in identifying potential cyber-attacks, understand their responsibilities and know how to report them to the right people in the organisation.

Key Takeaways

The insurers experience demonstrates that cyber security is not a technology problem with a technology solution. It is an organisational risk that requires a coordinated response across people, process, and technology, sustained over time with a foundation in rigorous measurement and improvement.

The decision to begin with a Broad Security Review before committing to specific technical improvements proved transformative. The insurer had a unified, evidence-based picture of the organisation's security maturity. This baseline did not merely identify problems; it enabled remediation prioritisation and investment allocation. Purple Teaming enabled the insurer to understand with independent experts where they were most at risk of attack and how to close the potential gaps in their SOC team. InfoSec training enabled them to educate staff members who are likely to be attacked of the risks and how to take action to keep the organisation secure and resilient against attack.

The decision to partner with Cyberfort for all three service streams proved pivotal. It provided the insurer with capabilities and objectivity that could not have been replicated internally, at a speed and cost that aligned with the urgency of the risk environment. Critically, the programme demonstrated that broad review, technical controls, and human behaviour must be addressed as a unified system, each reinforcing the others.

For insurers operating in complex, multi-jurisdictional environments, the question is no longer whether to invest in advanced cyber security, the regulatory and competitive pressures make this inevitable. The question is where to start, and how to ensure each investment builds on the last. The insurers results make a compelling case for starting with a comprehensive security review, and for partnering with specialists who can deliver the full breadth of services needed to act on what they find.

"Cyberfort's security experience and knowledge of the global insurance marketplace meant they were able to test our systems, processes, and people against industry benchmarks. The reports they produced and the InfoSec training programme they have put in place have helped us to identify potential risks, and put in place plans to address gaps which exist. By working with Cyberfort we have improved our cyber resilience posture."

Customer Feedback