PTS HELPS A GLOBAL INSURANCE GIANT TO UPLIFT THEIR SECURITY MATURITY ACROSS APAC

HOW PTS HELPED THEIR CLIENT PROTECT THEIR CUSTOMER DATA

We live in a world in which digital threats are becoming increasingly sophisticated and high-profile hacks regularly make the news.

That's why ironclad cybersecurity and robust data protection have never been more critical.

This was the challenge faced by a multinational insurance group, which recognised the growing sophistication of cybercriminals and the potential consequences of inadequate security measures.

First and foremost the client wanted to do the right thing by their customers, by ensuring no stone was left unturned to protect their data.

At the same time, the insurance group feared that a significant breach could:

- Inflict lasting damage to their reputation
- Trigger a client exodus
- Lead to heavy regulatory penalties and substantial remediation costs

---

To address the security challenges faced by the insurance company, PTS led a comprehensive multi-year security transformation programme that improved the client's overall security posture, and thus their security maturity.

This programme was proactive – measures were taken to get ahead of problems before they occurred.

Flexibility was another important feature – regular assessments were conducted to allow PTS to adapt the programme to evolving threats and technology advancements.

THE SIX BIG CHALLENGES PTS OVERCAME

PTS had to overcome six major challenges to successfully deliver on the programme objectives:

1. THE SIZE AND SCOPE OF THE PROJECT

Because this was a vast, multi-year project, we couldn't do everything all at once. So we had to prioritise cyber risks based on their potential impact on the client and their customers.

2. A COMPLICATED TECHNOLOGY ECOSYSTEM

The client had a mishmash of legacy and modern IT systems, with different vulnerabilities and security protocols. This made the company more susceptible to cyber attack.

3. NUMEROUS POTENTIAL VULNERABILITIES

The client had diverse operations across multiple countries, with many integrated environments and interconnected systems. This increased the number of potential vulnerabilities.

4. ONEROUS TRAINING DEMANDS

We had to educate numerous staff – across different departments, teams and countries – not only about specific security best practices but also the big picture around cybersecurity. That's because cybersecurity depends as much on human behaviours as technology.

5. COMPETITIVE PRESSURES

The client had to balance getting new products and/or services to market quickly with taking the time to ensure they had no security vulnerabilities.

6. EVER-EVOLVING SECURITY THREATS

The cyber threat landscape continued changing throughout the project, with attackers growing ever more sophisticated.

THE FIVE WAYS PTS TRANSFORMED THE SECURITY ENVIRONMENT

In partnership with our multinational insurance client, PTS implemented a proactive and comprehensive multi-year security transformation programme.

To ensure the program's success, we collaborated closely with the client's IT teams, risk management staff and executive leadership, which were spread across different countries.

This programme had five main priorities ...

1. STRENGTHENING CORE INFRASTRUCTURE

To strengthen the client's core infrastructure, they reduced the attack surface by identifying all the different infrastructure components and then consolidating them down.

For example, they consolidated data centres to reduce potential vulnerabilities and streamline operations. They also consolidated active directories to reduce complexity, minimise potential access points and strengthen overall security.

The company also implemented next-generation firewalls, such as Imperva, to bolster their ability to detect and prevent sophisticated cyber threats.

2. SIMPLIFYING INTERNAL SYSTEMS

The client conducted a comprehensive audit of all their applications and infrastructure, and then decommissioned the unnecessary and outdated ones. This simplification process:

- Minimised the overall attack surface
- Eliminated potential points of vulnerability
- Reduced inefficiencies within the business

3. MIGRATING TO THE HYBRID CLOUD

For security and efficiency reasons, we prioritised migration to the hybrid cloud, reducing the client's reliance on traditional on-premises infrastructure.

4. CONDUCTING ONGOING UPGRADES

The client implemented a continuous upgrade programme to ensure that systems and software remained up-to-date with the latest security patches and updates.

5. ENHANCING CYBER SECURITY

To detect and respond to security incidents promptly, the client introduced enhanced logging and monitoring mechanisms.

To strengthen security education and awareness, the company:

- Conducted more phishing simulations
- Organised more employee training programmes

THE PROGRAMME'S CRITICAL SUCCESS FACTORS

One of the main reasons the security transformation programme was so successful was because PTS was able to build a strong relationship with the client.

Through prior experience of a combination of PTS' skill, experience and collaborative approach, the client had the confidence to embrace the programme and ensure it was followed through to implementation.

This teamwork and leadership was reflected in seven ways ...

1. COMPREHENSIVE PLANNING

We created a detailed roadmap for the programme, which meant it had a clear, structured approach from start to finish.

2. THOROUGH STAFF ENGAGEMENT

We secured buy-in from senior leadership and key stakeholders, by actively engaging with them through workshops, showcases and presentations, and effectively communicating the importance of the programme.

3. STRATEGIC STAFF TRAINING

Whenever the need arose, we conducted targeted training sessions for the client's teams.

4. COUNTRY-SPECIFIC SOLUTIONS

We tailored our approach to suit the different cultural, regulatory and compliance environments in the client's different countries.

5. CULTURAL SENSITIVITY

We overcame cultural and language barriers by promoting open communication and cross-cultural collaboration.

6. ONGOING MONITORING

We regularly monitored the programme's progress, to ensure it remained on track and we could make adjustments if necessary.

7. OBJECTIVE MEASUREMENT

We proved the success of the programme through quantifiable metrics around improved security, reduced vulnerabilities and enhanced incident response capabilities.