itlab ANONYMISED CASE STUDY:

A Strong Partnership for a Secure Environment

Summary:

Client: ACME Insurance

Sector: Insurance

Company Size: 500+ Staff

IT Lab Services Provided: Managed Assurance Service (MAS) – a quarterly security service conducted over one year.

Managed Assurance Elements (MAS) include:

- Open Source Reporting (OSINT) – an intelligence assessment to identify risks
- Social Engineering - via email phishing campaigns and physical assessments
- Online Security Awareness Training
- Vulnerability Scanning
- Cyber Essentials (CE) Health Check
- Cyber Essentials PLUS assessment and certificate

Background:

ACME Insurance is acutely aware of the growing cyber threats to their business. The consequences of a cyber-attack could be devastating: operational downtime, fines, and – most feared of all – loss of customer trust.

They guard their reputation – built over a century – fiercely. In ACME's heavily regulated industry, compliance with bodies, including the Financial Conduct Authority (FCA), the Prudential Regulation Authority (PRA) and the Information Commissioner's Office (ICO), is paramount.

ACME was alarmed by the regular appearances in the press of high-profile data breaches and the explosion in phishing attacks. Following a minor security scare of their own, they identified that their employees presented the main risk to their security. Consequently, ACME decided on a strategy to make its users their best line of defence – not their weakest link. Everyone - from their call centre staff to their CEO - had a crucial role to play.

They also wanted to build their security credentials to reassure their stakeholders and customers they were in safe hands. ACME has limited security expertise in-house and turned to us as their trusted partner. For obvious reasons, we're protecting their identity.

ACME is a long-standing IT Lab client; our partnership began when we helped them to migrate from their legacy applications to the cloud. Today, our services include IT support for their 500-strong user-base.

We proposed a bespoke Managed Assurance Service (MAS) to:

- Improve the security awareness of all employees, including the c-suite.
- Identify the main areas of risk across ACME's infrastructure and provide a clear road-map for remediation.
- Enable ACME to show their commitment to security by attaining Cyber Essentials PLUS.
- Deliver continuous assurance for their internet facing systems, allowing new external vulnerabilities to be quickly identified and fixed.

> "As MAS is conducted over 12 months, we didn't feel overwhelmed by the amount of work to do - IT Lab guided our priorities as well as identifying our risks. They helped us with the remediation work and are incredibly supportive. Culturally, there's been a sea change; our users are much more security savvy, and our vulnerabilities are reviewed at every board meeting. We were delighted to pass Cyber Essentials PLUS first time and we're considerably more confident and informed than we were a year ago."
>
> - IT Director, ACME Insurance

Navigate:

Plotting a Course for Better Security with MAS

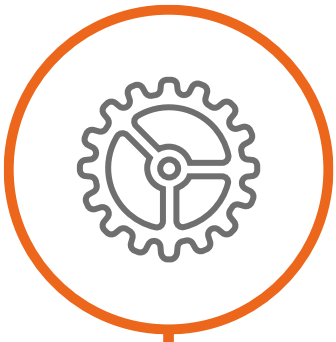
Our tried and tested process was sympathetic to our client's time, with minimal impact on their business operations. To achieve ACME's objectives, we embarked on:

- A reconnaissance mission to gain an intimate understanding of ACME's existing security posture.
- A physical security review to assess not just technical controls but the 'people aspect' of physical security.
- A deep dive into public sources to ascertain if sensitive information was exposed.
- Employee interviews – from the top down - for insights into ACME's starting levels of security awareness.
- An audit of all business-critical systems; maintained by IT Lab and third-parties. This included on-premise systems, cloud-based systems and all user endpoints, e.g. workstations and mobiles.

During the exercise, elements of ACME's infrastructure were in flux; some systems were being changed or updated. Our flexible cybersecurity team adapted their approach to ensure the project wasn't compromised.

The resulting report was presented to ACME's leadership, internal systems teams and head of IT. It was in plain-English with additional technical information for IT personnel.

> "Our cyber team, alongside our dedicated onsite engineer, worked closely with ACME to identify pain-points and highlight the main areas of risk and their possible consequences. We designed and executed a comprehensive service which is rapidly improving their security posture.
>
> Stephen Rivers, IT Lab's Account Manager for ACME Insurance"



Integrate:

Weaving MAS Into the Fabric of the Business

To enable ACME to achieve and maintain a baseline of cybersecurity, **every quarter** IT Lab:

- Ensures their external infrastructure is secure by running comprehensive vulnerability scans.
- Benchmarks employee cybersecurity awareness via email phishing assessments and online security awareness training, building knowledge throughout the year.
- Confirms that end-user devices, including laptops, desktops and mobiles, are built and maintained securely through auditing and vulnerability scanning.
- Performs gap analysis assessments to map ACME's progress and check their readiness for their Cyber Essentials PLUS assessment.
- In quarter 3, we conducted a Cyber Essentials Health Check to review our client's progress and check their readiness for their CE PLUS Assessment in the final quarter.

— In quarter 4, we conducted a Cyber Essentials PLUS assessment. Perspective Risk – an IT Lab company – is a CREST Cyber Essentials Certification body which means we can perform Cyber Essentials PLUS assessments and issue certificates.

Operate:

How MAS Benefits ACME Today

By assessing and testing ACME's security posture and controls across its people, technology and infrastructure, the company has significantly reduced the likelihood of a successful cyber-attack. The risks to ACME's external infrastructure are down by approximately 75%.

ACME enjoys a marked improvement in the security awareness of its employees. Before the project, nearly 11% of users fell for a basic phishing (hoax) email, which exposed their machines – and consequently ACME's internal network - to compromise and disruption. Security awareness training, as part of our customised MAS service, includes four levels of phishing tests, from low to high sophistication. In quarter 3, a test phishing email with the highest level of complexity succeeded in duping only 2% of staff.

Staff training, bolstered by a combination of other MAS measures, has allowed ACME to meet a baseline level of security. Ten months into the project, they were proud to achieve Cyber Essentials PLUS.