8Depths

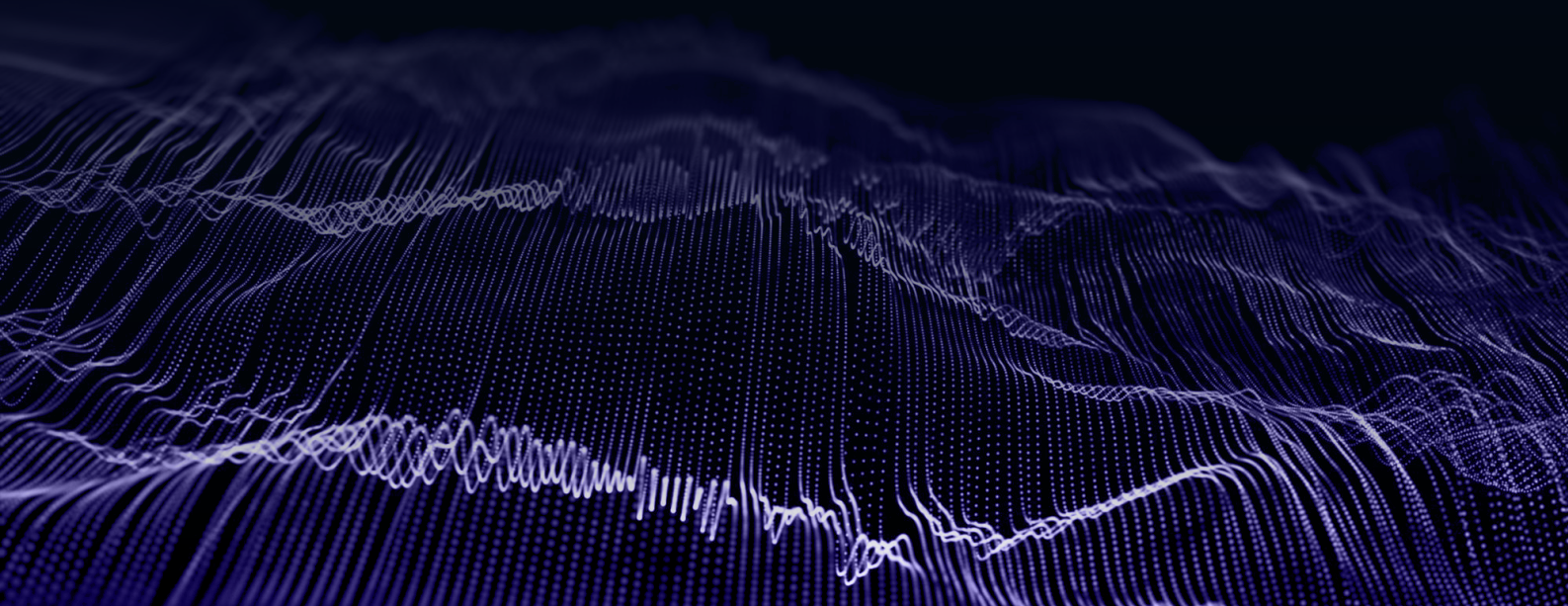
Are You Truly Seeing a Return on Your Cyber Security Investment?

Most organisations are spending more than ever on cyber security. **But few can confidently answer one critical question:**

Is that expenditure actually delivering value —or simply exacerbating a cycle of cost?

Explore the hidden financial reality of cyber security and why many organisations unknowingly fund an ever-expanding cost loop.

www.8depths.com



1 The start of your journey: Tools and Services

Every journey starts with the right intentions—investing in security tools, platforms, and managed services to protect the business and meet stakeholder expectations. Over time, however, these investments multiply. New solutions are layered on top of existing ones, often with overlapping capabilities and increasing operational complexity. What begins as strategic enablement can quickly evolve into fragmented spend—where costs rise, but measurable risk reduction remains unclear.

2 Validation Through Compliance

With technology in place, you seek validation. Certifications and frameworks such as ISO 27001, SOC 2, PCI DSS, and Cyber Essentials Plus become essential markers of trust. Achieving these standards requires audits, consultancy, and ongoing internal effort. Maintaining them requires even more; while compliance strengthens credibility, it does not guarantee security—yet the cost of maintaining your security continues to grow.

3 Transferring Risk with Cyber Insurance

To further mitigate exposure, you invest in cyber insurance. Policies provide reassurance—on the surface. But premiums increase, requirements become more stringent, and coverage is often conditional. In many cases, additional expenditure is required just to remain insured. And when an incident occurs, payouts are not guaranteed—often dependent on whether your controls meet strict post-incident audit criteria.

At This Point, It Looks Like You're Covered:

- **Digital assets secured**
- **Security posture validated**
- **Financial liability transferred**

Yet the reality is different.

Even well-funded, fully-certified organisations are still being compromised.

4 The Ransom Decision

When an attack ambushes you, the situation escalates immediately. A ransom demand presents a critical decision—pay or refuse. Neither option is favourable. One risks regulatory scrutiny and consequences, the other risks operational and reputational damage. Despite your expenditure, you are left managing outcomes—not preventing them. The very controls designed to prevent this moment now are insufficient against its reality.

5 The Cost of Incident Response

The aftermath introduces urgency and significant cost. Incident response is complex, involving digital forensics, root cause and impact assessments, data exfiltration investigation and recovery service. Specialist expertise is required, often at rates starting from £1,500 per day, with engagements lasting weeks. Each day exposes more gaps and more cost—raising a sharp question: why didn't previous investments prevent this?

6 Regulatory Exposure

Regulatory scrutiny follows quickly. Authorities assess not how much you spent—but how effective those measures proved. Fines in the UK ranged from £60,000 to £20 million (ICO), up to £11 million (FCA), and even higher globally. Significant investment does not guarantee protection from penalties—it often increases expectations.

7 Legal and Compensation Costs

If data is exposed publicly, the financial impact deepens. Legal action, group litigation, and compensation claims can follow. You may be required to fund settlements, legal defence, and ongoing support for affected individuals—including credit monitoring and identity protection. These costs extend long after the incident, compounding the total financial burden.

8 Recovery, Remediation and Lost Revenue

Recovery is rarely straightforward. Systems must be rebuilt, infrastructure replaced, and operations restored. This requires time, resources, and further investment—while your business continues to experience disruption. Revenue is lost. Customer confidence declines. The impact extends beyond IT into the core of the organisation. The cost is not just technical—it is commercial, operational, and reputational.

The Bigger Picture

At every stage, organisations are paying to:

Each layer is designed to reduce risk—yet together, they often create a continuous cycle of expenditure.

So the question remains: **where is the RETURN ON INVESTMENT?**

More importantly—is there a smarter, more effective way to approach cyber security spending?

Contact Us

Reach out to an 8Depths team member to uncover how leading organisations are rethinking cyber security investment – and how you can do the same.

8depths.com/contact

+44 (0) 20 4617 9888

info@8depths.com

*Note: The views and opinions included in this report belong to 8Depths and are based on current, subjective assessments. They do not necessarily mirror the views of any external entity. While we aim for accuracy, these viewpoints are for informative purposes only and do not constitute a guarantee of future outcomes.