Business Case: Strengthening Organizational Resilience Through BJSL Training Cyber Security Training

This business case evaluates the investment in BJSL Training for an initial cohort of 10 employees. By transitioning staff from "potential vulnerabilities" to "active defenders," the organization creates a sustainable **Human Firewall**.

---

1. Executive Summary

Cybersecurity is no longer just an IT issue; it is a core business risk. With **68% to 82% of all data breaches** involving a human element, technical defences alone are insufficient.[1] This proposal outlines two pathways for training 10+ workers to mitigate these risks, ensure GDPR compliance, and protect the company's financial and reputational standing.

---

2. Financial Investment Options

The following options allow the organization to tailor training based on staff technical proficiency:

Option	Target Audience	Cost per Person	Total (Min. 10)
Foundation Bootcamp (2-Day)	General office workers; no prior experience required.	**£695**	**£6,950**
Condensed Course (1-Day)	Proficient users, Project Managers, or Team Leads.	**£495**	**£4,950**

Note: Both courses cover identical subjects, but the condensed version is higher intensity for faster learners.

---

3. The Problem: The Cost of Inaction

The risk of not training staff is significant and measurable:

- **Average Breach Cost**: In 2025, the average cost of a data breach for a UK SME reached **£75,000** per incident.[2] For larger organizations, this figure can escalate to **£3.29 million**.[3]

+1

- **Phishing Dominance**: **91% of cyberattacks** start with a phishing email—a threat specifically addressed in the BJSLO curriculum.[4]
- **Hidden Costs**: Beyond immediate financial loss, breaches result in **reputational damage**, loss of customer trust, and potentially massive **GDPR fines** (up to 4% of annual revenue).[5]

---

4. Proposed Solution: The BJSL Training Curriculum

The training specifically targets the most common entry points for attackers as outlined in the course syllabus:

- **Social Engineering Defence**: Identifying "quishing" (QR code phishing), vishing, and impersonation.
- **Secure Remote Working**: Training specifically for cloud services and mobile device security, critical for modern hybrid workforces.
- **Regulatory Alignment**: Ensuring staff understand organizational and legal compliance (GDPR).

---

5. Return on Investment (ROI)

- **Risk Reduction**: Regular training can reduce an organization's risk profile from **60% to 10%** within the first year.[6]
- **Cost Savings**: Organizations with comprehensive awareness programs report average savings of **$1.5 million** per breach compared to those without.[7]
- **High Payback**: Even the least effective training programs show a **7-fold ROI**, while high-performing programs can yield a **37-fold return**.[8]

---

6. Long-Term Strategy: Maintaining the Human Firewall

To ensure the benefits of this training are not lost over time, the company should implement the following "Continuous Education Strategy":

1. **Tiered Learning Path**: Use the **2-Day Bootcamp** as the mandatory baseline for all new hires and general staff. Use the **1-Day Condensed Course** for rapid upskilling of technical managers and "Security Champions."
2. **Monthly Micro-Learning**: Since awareness starts to fade after 4 months, implement monthly **"bite-sized" 10-minute refreshers** on new threats like AI-generated deepfakes.[9]
3. **Security Champions Program**: Designate the trained Project Managers as internal "Champions" to provide peer-to-peer guidance and maintain a "Security-First" culture.
4. **Phishing Simulations & "Just Culture"**: Run regular, non-punitive phishing tests.[10] Foster a "Just Culture" where employees are **rewarded for reporting** suspicious activity rather than being blamed for mistakes.[11]

+1

5. **Performance Metrics**: Track the "Reporting Rate" (how many employees flag threats) versus the "Click Rate."[12] A healthy firewall shows a steady increase in threat reporting over time.

Conclusion

An investment of **£4,950 to £6,950** is a negligible cost compared to a potential **£75,000+** loss from a single breach. By training these 10 individuals, the company initiates a shift in culture that protects its data, its people, and its future.

Next Step: To book either of these cohorts, you can contact the BJSL Training team at **01932 949059** or via email at **Adrian@bjsl.uk .** Schedule your first cohort now.