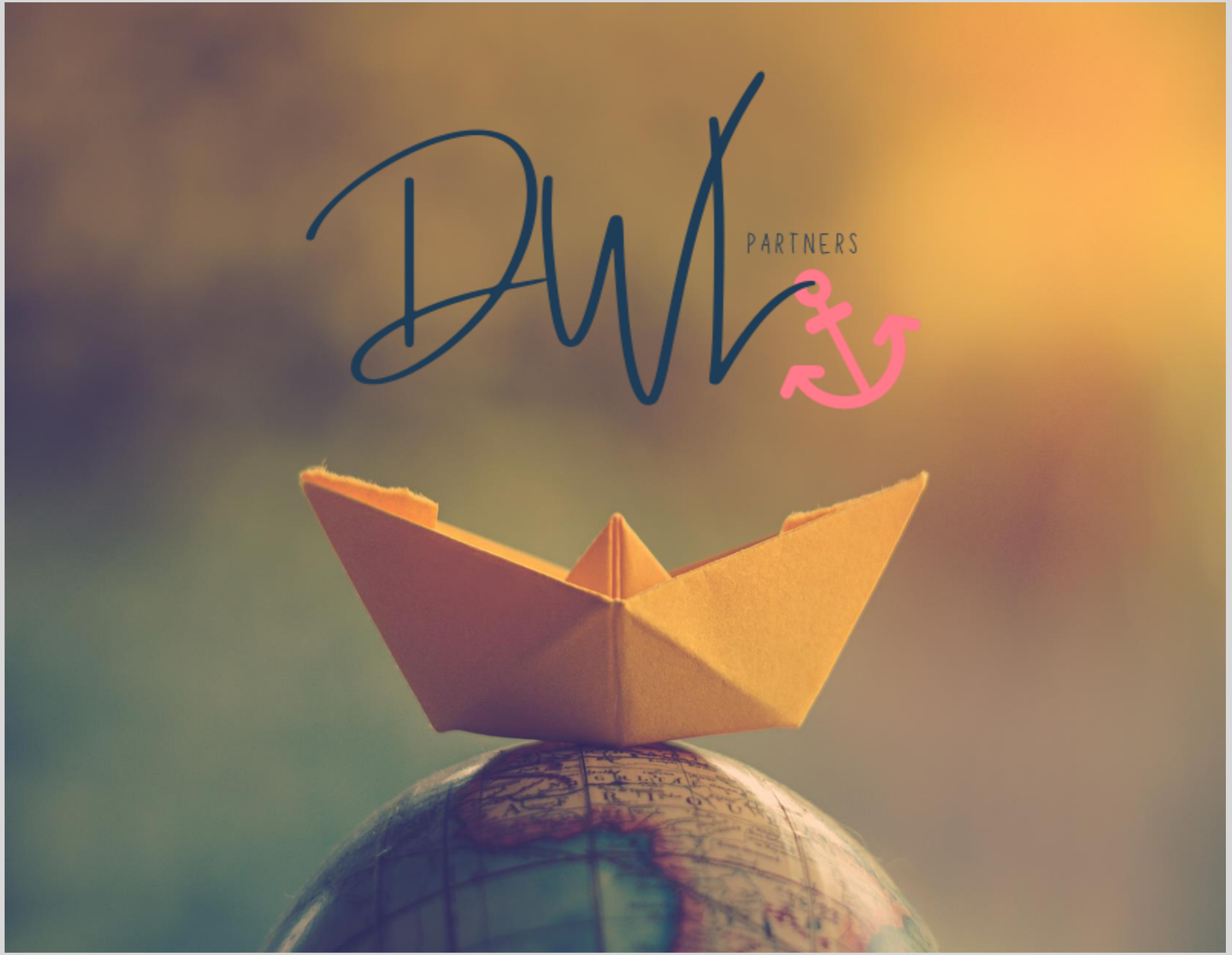
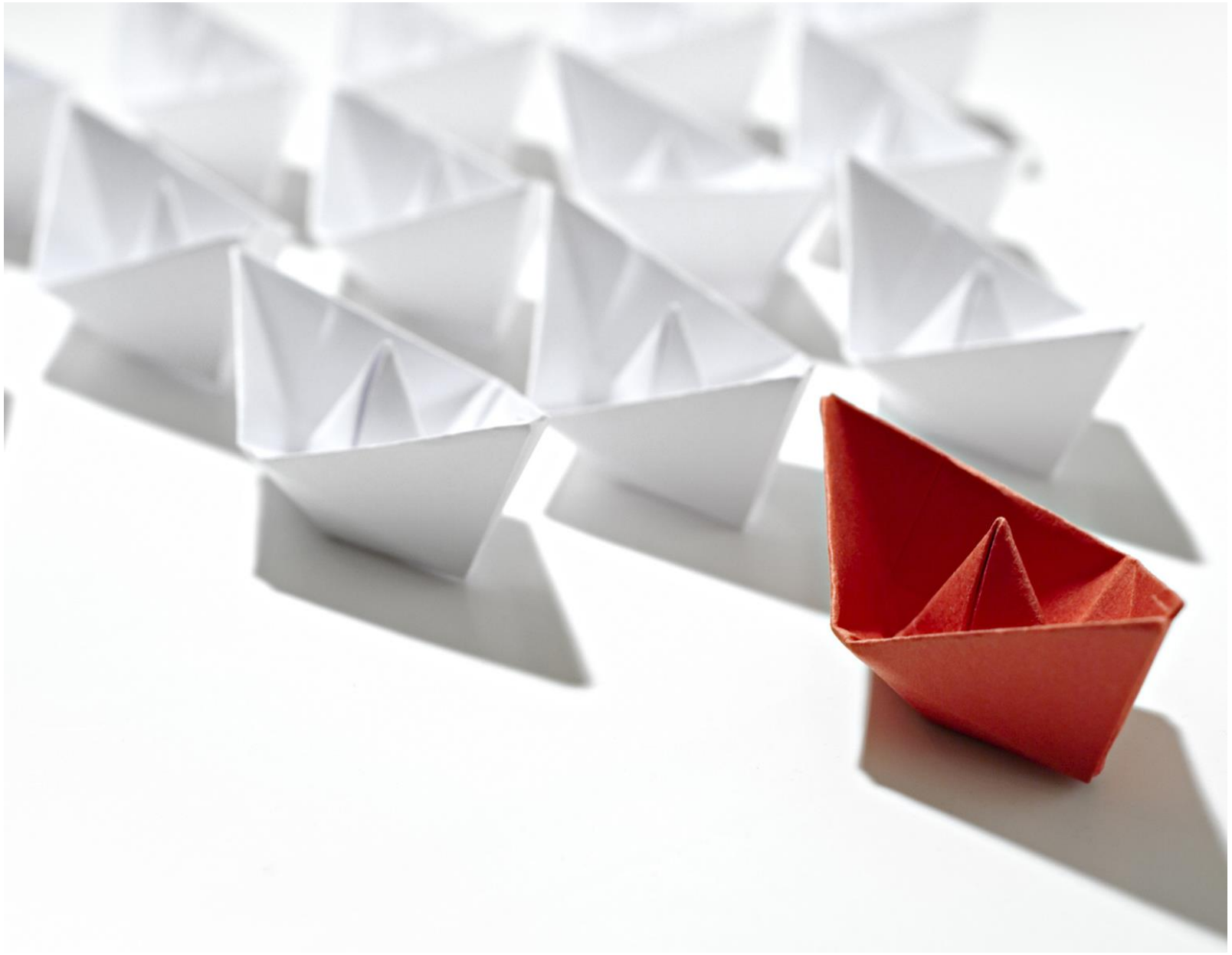



# SME CYBER SECURITY

SIMON BROWNHILL



# ABOUT DWL PARTNERS

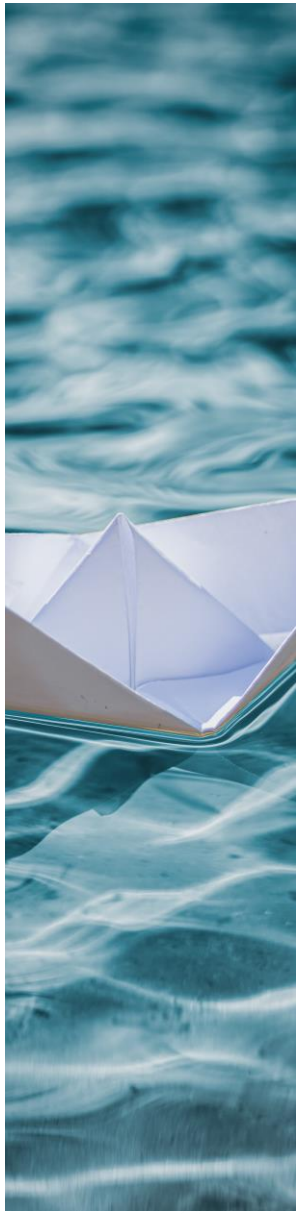
# ABOUT DWL PARTNERS LIMITED

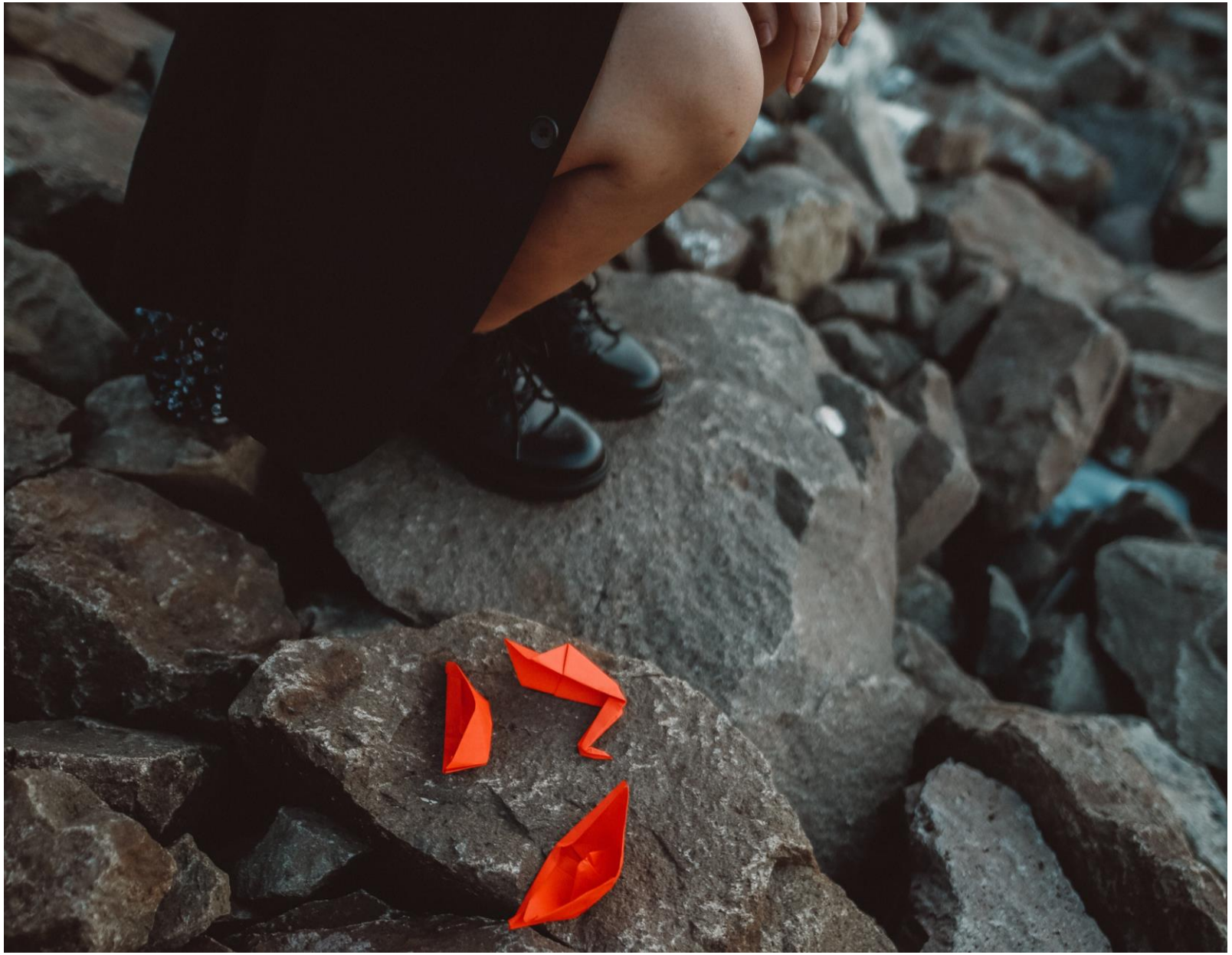
DWL Partners is a leading consulting firm that helps organisations stay ahead of the game in the fast-changing world of cybersecurity and technology transformation. With a team of experienced and versatile experts, DWL Partners offers a range of services, such as:

- Cybersecurity strategy and governance
- Threat management and security operations
- Risk assessment and compliance
- Technology transformation and innovation
- Program and project management
- Business analysis and change management
- Stakeholder engagement and communication
- DPO as a service

DWL Partners has over 30 years of experience in delivering successful outcomes for clients across various industries and regions.

We pride ourselves on our long-term and trusted relationships with clients, stakeholders, and vendors.





# CYBER OVERVIEW

# WHY IS THIS IMPORTANT TO ME?

- The importance of cyber and information security for SMEs
  - SMEs are increasingly targeted by cybercriminals.
  - The financial, reputational, and operational impacts of cyber incidents.
  - Compliance with regulations and customer trust.

## Small businesses (less than 1,000 employees)

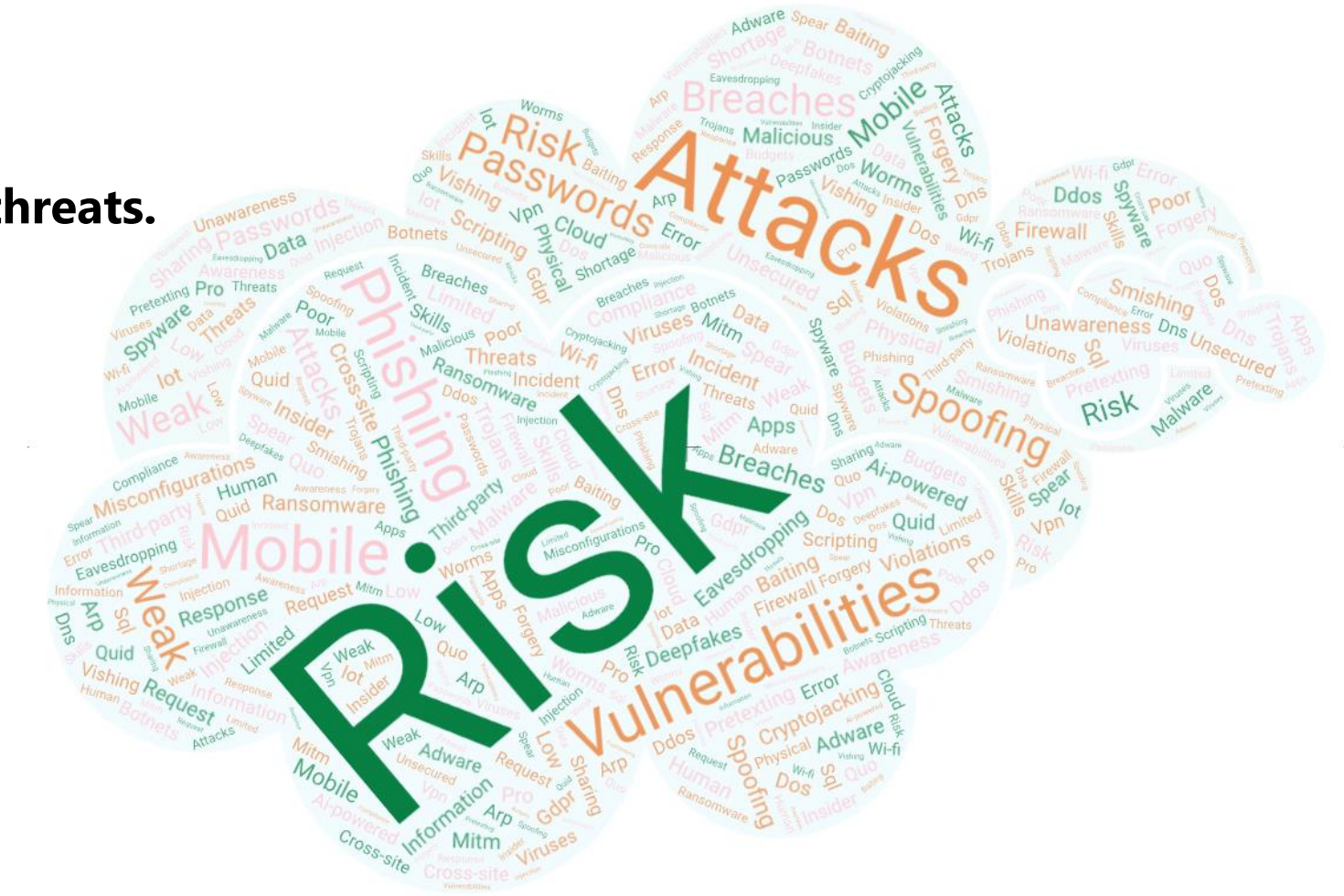
| | |
|---|---|
| **Frequency** | 699 incidents, 381 with confirmed data disclosure |
| **Top patterns** | System Intrusion, Social Engineering and Basic Web Application Attacks represent 92% of breaches |
| **Threat actors** | External (94%), Internal (7%), Multiple (2%), Partner (1%) (breaches) |
| **Actor motives** | Financial (98%), Espionage (1%), Convenience (1%), Grudge (1%) (breaches) |
| **Data compromised** | Credentials (54%), Internal (37%), Other (22%), System (11%) (breaches) |

**REALLY?**

Source: Verizon DBIR https://www.verizon.com/business/resources/reports/dbir/2023/small-business-data-breaches/

# WHAT ARE THE THREATS?

- **Overview of common cyber threats.**
  - Phishing attacks
  - Ransomware
  - Insider threats
  - Data breaches
  - Supply chain attacks



# WHAT DO I NEED TO CONSIDER - AI AND THE LIKE?

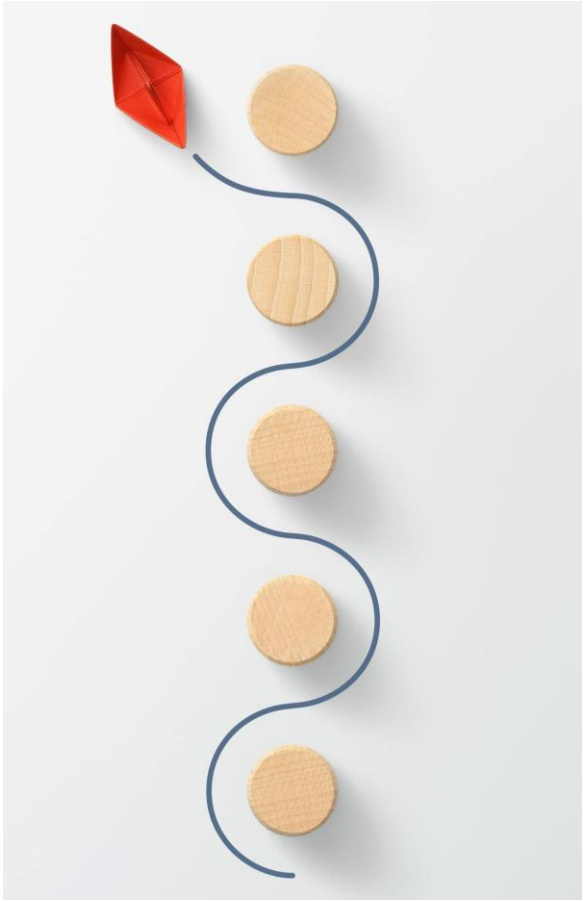
- Data dependency – Limited data, quality and data silos
- Ethical constraints and bias – Unintentional bias, lack of transparency and job displacement
- Security and privacy – Data breaches, adversarial attacks, and compliance challenges
- Expertise and awareness – Skills gap, Limited understanding and integration issues

# DEVELOPING AN EFFECTIVE CYBER/INFORMATION SECURITY STRUCTURE

- Cyber 101- Risk Assessments (if you can’t measure it, how do you know how to protect it)
- Customised remediation, strategies and roadmaps
- Collaborative implementation and technical expertise
- Continual improvement

# CYBER FRAMEWORKS

- Cyber Essentials – standard and plus
- ISO 27001
- DORA and FCA 21/3
- And the list goes on…



# EMPLOYEE AWARENESS

IMPORTANCE OF TRAINING AND AWARENESS PROGRAMS

CREATING A SECURITY-CONSCIOUS CULTURE

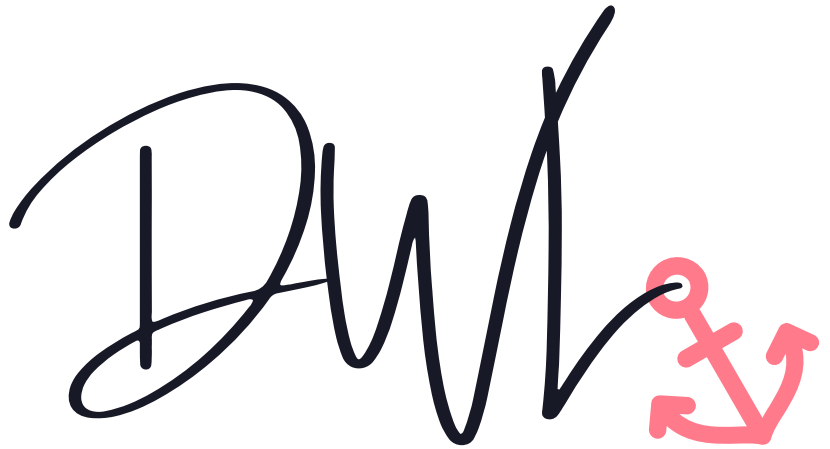
REGULAR UPDATES AND REFRESHER COURSES

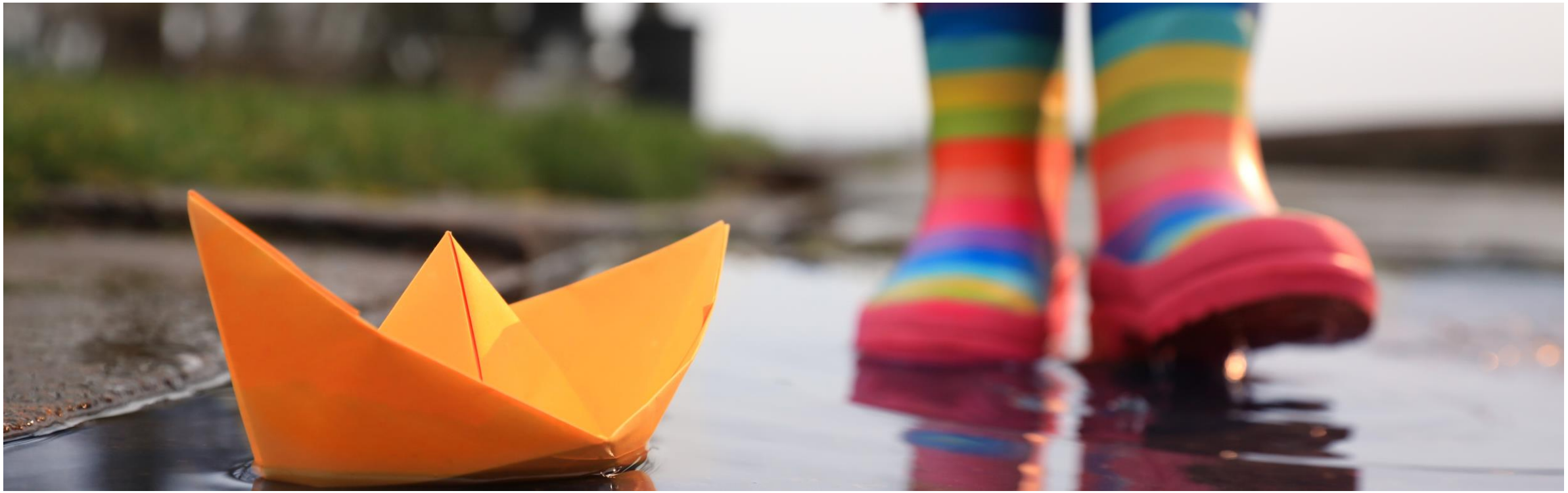
# INCIDENT RESPONSE

- Steps in an incident response plan (preparation, identification, containment, eradication, recovery, lessons learned)
- Importance of having a playbook and regular drills
- External resources and support (e.g., incident response consultants, NCSC)

# GOOD SOURCES FOR ASSISTANCE

- National Cyber Security Centre (NCSC)
- Information Security Forum (ISF)
- Cybersecurity and Infrastructure Security Agency (CISA)
- European Union Agency for Cybersecurity (ENISA)





# QUESTIONS

Thank you