Stone Business Consultancy
Monthly Seminar Running Sheet
Seminar Topic: Cybersecurity for Small Businesses

Seminar Overview

The first Stone Business Consultancy seminar for 2026 focused on **cybersecurity risks and protection strategies for small businesses**. The session was designed to increase awareness of the most common cyber threats affecting small operators and to provide practical, low-cost actions that can be implemented immediately.

The seminar combined education, practical examples, and open discussion, with a strong emphasis on prevention, access control, and protecting business data and digital assets.

Key Themes and Discussion Areas

1. The Current Cyber Threat Landscape for Small Business

The seminar opened with an overview of why small businesses are increasingly being targeted by cybercriminals. Key points included:

- Small businesses are often seen as **easy entry points** due to limited IT systems and fewer security controls.
- Attacks are usually **automated and opportunistic**, not personal.
- The financial, operational, and reputational damage from a breach can be significant.

Participants were introduced to the concept of:

- **Primary attacks –** Directly targeting the business.
- **Secondary attacks –** Gaining access through connected individuals, suppliers, or related accounts.

This reinforced the idea that cybersecurity is not just a **technical issue**, but a core **business risk management priority**.

---

2. Common Types of Cyber Attacks

The session explored the most frequent attack methods affecting small businesses:

Phishing

- Fraudulent emails or messages designed to trick users into clicking links or providing login details.
- Often impersonate trusted organisations or known contacts.
- Typically create urgency (e.g. payment required immediately).

Fake Invoicing & Payment Redirection

- Interception or imitation of legitimate invoices.

- Requests to change bank details.
- Highly effective where verification processes are weak.

Data Theft

- Unauthorised access to business systems or cloud storage.
- Extraction of customer, financial, or operational data.

Ransomware

- Locking a business out of its own systems.
- Demanding payment for data recovery.
- Particularly damaging where backups are not in place.

The discussion emphasised that **human behaviour is the most common entry point**, not system failure.

---

3. Password and Access Management

A significant portion of the seminar focused on improving password security.

Best practice principles:

- Use **long, strong, and unique passwords** for every system.
- Avoid reusing passwords across platforms.
- Do not store passwords in physical notebooks or unsecured files.

Password managers were recommended as the most secure and practical solution for:

- Storing credentials
- Generating strong passwords
- Managing multiple business logins

The importance of **separating personal and business accounts** was highlighted to prevent personal breaches from compromising business systems.

---

4. Two-Factor Authentication (2FA)

Two-factor authentication was presented as one of the **highest-value, lowest-cost security measures**.

Benefits:

- Prevents access even if a password is stolen.
- Essential for:
  - Email accounts
  - Social media
  - Accounting software
  - Cloud storage
  - Banking platforms

Participants were encouraged to prioritise enabling 2FA on all critical systems.

---

5. Social Media and Digital Asset Protection

The seminar addressed the growing risk of business social media accounts being taken over.

Key controls discussed:

- Limit the number of users with **full admin access**.
- Maintain a **backup admin account** for recovery purposes.
- Use **clear and consistent business branding and usernames** to reduce impersonation risk.
- Consider **account verification options** where appropriate.

These measures help ensure continued access to business pages and protect advertising accounts and customer communication channels.

---

6. Recognising Red Flags

Participants were guided through practical warning signs of cyber threats:

- Unexpected links or attachments
- Email address changes in payment requests
- Messages that create urgency or fear
- Slight variations in domain names
- Unusual login alerts

The key message was to **slow down and verify before acting**, particularly when money or sensitive data is involved.

---

7. Data Protection and Business Continuity

Cybersecurity was positioned as part of broader business continuity planning.

Essential practices:

- Regular, automated **data backups**
- Keeping **software and systems updated**
- **Staff awareness and training**
- Avoiding sensitive work on **public Wi-Fi**

Backups were emphasised as the primary recovery tool in the event of ransomware or system failure.

Practical Implementation Focus

Throughout the session, the emphasis remained on:

- Affordable

- Simple
- Immediately actionable

security improvements suitable for sole traders and small teams without dedicated IT support.

Participants were encouraged to adopt a **step-by-step implementation approach**, starting with:

1. Password security
2. Two-factor authentication
3. Backup systems
4. Access control reviews

Key Takeaways for Small Business Owners

- Cybersecurity is a **business responsibility**, not just an IT issue.
- Most attacks are **preventable with basic controls**.
- Email and social media accounts are **critical infrastructure** for small businesses.
- Access management is one of the **biggest risk areas**.
- Backups are essential for operational survival.

Next Steps and Follow-Up Actions

The following actions were identified:

- A **cybersecurity checklist** will be distributed to support implementation.
- Seminar resources and de-identified notes will be made available.
- Participants were invited to provide feedback via the review link.
- Registrations are open for the **next seminar on 19 March**, which will focus on practical AI applications for small business.

Conclusion

This seminar provided small business owners with a clear, practical understanding of the current cyber threat environment and the simple measures that significantly reduce risk.

The session reinforced that effective cybersecurity is built on:

- Strong access controls
- Consistent verification processes
- Regular backups
- Ongoing awareness

rather than complex or expensive technology.

The overall focus was on giving participants the confidence and tools to take immediate action to better protect their businesses in an increasingly digital operating environment.