COMPLIMENTARY WEBINAR FOR UK GOLF FEDERATION MEMBERS

Building a Cyber-Resilient Golf Club

Protecting operations, member information and organisational confidence

Golf clubs now depend on connected services for email, Microsoft 365, membership records, tee bookings, payments, hospitality, finance and day-to-day communication. That dependence brings efficiency, but it also means that an affected account, workstation or supplier connection can quickly disrupt club operations and place sensitive information at risk.

Cyber resilience is therefore broader than antivirus or a single security product. It combines protected identities, securely managed devices, informed users, active monitoring, tested backups, clear incident responsibilities and evidence that controls are working. This webinar uses the Resilience 360 approach to connect those elements and help clubs identify proportionate, practical priorities.



Could your club answer these questions today?

- Are Microsoft 365 identities and email properly protected?
- Are club workstations supported, updated and monitored?
- Would staff recognise a convincing payment or login scam?
- Can essential systems and information be recovered?

EVENT DETAILS

Date: 01/12/2026

Time: 14:00 – 15:00

Online platform: Microsoft Teams

Speakers: Gregoy Olczyk

Registration link / QR code: Click Here

A practical, plain-English agenda

01

Cloud and Microsoft 365

Protect the identities and services through which club business is conducted. We will consider multi-factor authentication, administrator access, joiners and leavers, suspicious sign-ins, mailbox forwarding, external sharing, third-party access and the distinction between cloud availability and recoverability.

02

Workstations and devices

Understand the local technology layer: supported operating systems, prompt security updates, secure configuration, endpoint detection and response, encryption, administrative privileges, personally owned devices and the importance of maintaining an accurate inventory.

03

People and behaviour

Reduce everyday exposure to phishing, impersonation, fraudulent payment requests and unsafe information handling. The session will examine verification routines, password and authentication habits, rapid reporting and how a positive security culture improves detection without blaming users.

04

Response and recovery

Prepare for the point at which prevention is not enough. Define monitoring, decision-making and escalation; know how accounts or devices will be contained; protect evidence; communicate with staff and stakeholders; and regularly test that essential data and services can actually be restored.

05

Insurance readiness

Connect technology controls with clear, supportable evidence. We will consider the information insurers may expect around identity, endpoints, patching, backups, awareness and incident response, while reinforcing that insurance complements good resilience and does not replace it.

YOU WILL LEAVE WITH

- ✓ A joined-up view of club cyber risk
- ✓ Questions for technology and insurance providers
- ✓ Priorities across cloud, devices, people and recovery
- ✓ A practical resilience review checklist
- ✓ A clearer understanding of control evidence

WHO SHOULD ATTEND

- Club managers and general managers
- Board and committee members
- Finance and operations leaders
- Membership, marketing and communications teams
- People responsible for technology, information governance, risk

No specialist technical knowledge is required.

RESERVE YOUR COMPLIMENTARY PLACE

Educational session. Cyber-insurance content is general technology and governance guidance, not insurance advice.