heart of the south west
local enterprise partnership

Heart of the South West Local Enterprise Partnership

Finance & Resources

Report theme: Cyber Protection

Author: Eifion Jones

Summary

With the increase in cyber incidents across all sectors, this paper sets out the LEP's plans to mitigate this.

Recommendations

That F&R note the steps already taken and advise on any further proportionate measures

---

Background

Cyber breaches have received increasing coverage in recent months and in March Government's Cyber Security Breaches Survey[1] reported

- Four in ten businesses reported cyber security breaches or attacks in the last 12 months. This is higher among medium businesses (65%), large businesses (64%) and high-income charities (51%)
- Fewer businesses are identifying breaches or attacks than in 2020 with the decline greatest among small businesses, from 62% to 39%
- Among those that have identified breaches or attacks, around a quarter experience them at least once a week. The top 3 attacks are from phishing (for 83%), impersonation (27%) and virus/ malware (9%)
- The main impact reported from breaches are temporary loss of access to files or networks and disruption to websites, applications or online services. Whilst incidents viruses, ransomware, account takeovers, hacking attempts or other unauthorised access are rarer, the impact is more substantial
- The costs of security breaches ranges from £8,460 - £13,400, though other sources quote significantly higher amounts; IBM and Ponemon's international study states that data breaches cost UK enterprises an average of $3.88 million per breach

Mitigation

Historically the LEP has not handled large amounts of personal data though this is beginning to change with the recent Train4Tomorrow programme. The LEP has in place the following mitigation:

- The LEP has an information policy (attached) which details required levels of security in passwords on laptops and phones, protection in place etc. In August a training

[1] Cyber Security Breaches Survey 2021 - GOV.UK (www.gov.uk)

session was held for core LEP staff on this and the policy is being refreshed in conjunction with the LEP's IT support consultants

- LEP IT equipment is protected by anti-virus software, home routers have their own firewalls and all LEP files are held in SharePoint. No files are to be stored on laptops
- In prior years the LEP's public liability insurance provided a small amount of coverage – up to £20k costs – against a cyber incident. In common with other policies in the marketplace this was removed from the policy in the annual renewal in April and so the LEP has taken out specific cover to provide up to £2m of cover against a cyber breach, covering response/ hacking, extortion, business interruption, court attendances etc
- Through the Train4Tomorrow agreement, DWP are also requiring successful bidders to hold a Cyber Essentials accreditation and to achieve Cyber Essentials Plus by March. These National Cyber Security Centre schemes put in place further steps to help protect organisations and will be required by other Government departments where projects handle large amounts of sensitive data. The LEP will be working through these in the autumn at a cost of £300 for each scheme

Attachments

HotSW LEP
Information Securit