Security Best Practice in Business

Data Security

Best Practice in business

Cyber Security – Data Security

Just under half (46%) of all UK businesses identified at least one cyber security breach or attack in 2016. This rises to two-thirds among medium firms (66%) and large firms (68%). -UK Government Cyber Security Breaches Survey 2017.

Two Principles

Good Cyber Security in Business

- **Prevention**: Preventing a cyber-attack is about taking the necessary steps to avoid becoming the victim of an attack.
- **Recovery**: In the event of a cyber-attack, how well can the business recover? How resilient is the business in dealing with the aftermath of data loss? How quickly can they recover and limit the effects the attack has on the business?

Good practice

Protect against viruses, spyware, and other malicious code

- Make sure each of your business's computers are equipped with antivirus, antimalware software and antispyware, and update them regularly.

Secure your networks

- Use a firewall and encrypt information. If you have a Wi-Fi network, make sure it is secure and hidden. Password protect access to the router.

Establish security practices and policies to protect sensitive information

- Establish policies on how employees should handle and protect personally identifiable information and other sensitive data.

Educate employees about cyber threats and hold them accountable

- Educate your employees on online threats and how to protect your business's data, including safe use of social networking sites.

Good practice - continued

Require employees to use strong passwords and to change them regularly

- Consider implementing multifactor authentication that requires additional information beyond a password to gain entry.

Control physical access to computers and network components

- Prevent access or use of business computers by unauthorised individuals. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

Make back-up copies of important business data and information

- Back up critical data including: word processing documents, electronic spreadsheets, databases, financial files, human resources files and accounts. Back up data regularly and store the copies either offsite or on the cloud.

Employ best practices on payment cards

- Isolate payment systems from other, less secure programs, and do not use the same computer to process payments and surf the internet.

Good practice - continued

Create a mobile device action plan

- Require users to password-protect their devices, encrypt their data and install security apps to prevent criminals from stealing information while the phone is on public networks.

Protect all pages on your public-facing websites

- Not just the checkout and sign-up pages. This will help to protect against web-based attacks such as SQL injection.

UK Government: 10 steps recommendation

1. **Information Risk Management Regime** - Assess the risks, create and communicate a risk management policy
2. **Secure Configuration** - Remove or disable any unnecessary functionality from IT systems and keep them patched against known vulnerabilities
3. **Network Security** - Follow network design principles when configuring perimeter and internal network security. Filter and monitor traffic for unusual or malicious activity
4. **Manage User Privileges** - Grant users only enough access to allow them to carry out their job. Limit the number of administrator accounts and ensure that they are not used for high risk or day-to-day activities. Monitor user activity, particularly any access to sensitive information
5. **User Education & Awareness** - All users should receive regular training on cyber risk, with specialist training for those privileged roles, such as system administrators. Produce policies to describe acceptable use
6. **Incident Management** - Establish incident response procedures and test these regularly. Report online crimes to the relevant authorities.
7. **Malware prevention** - Scan for malware across the organisation. This should extend to include e-mail, web browsing, removable media and personally owned devices.
8. **Monitoring** - Continuously monitor inbound and outbound network traffic
9. **Removable Media Controls** - Control the use of removable media for transferring files. Scan all removable media devices on a standalone machine before any data is imported onto your system
10. **Home and Mobile working** - Train users on the secure use of their devices. Protect data on the device by using encryption, and protect data in transit by using a VPN

Scottish Government

Click Here for the:
Scottish Government published
Public Sector Cyber Resilience Plan

https://www.gov.scot/publications/cyber-resilience-strategy-scotland-public-sector-action-plan-2017-18/

Task – Now do Task 15