Guernsey Financial Services Commission

Self-Assurance Help Sheet Cyber Thematic

Please find below a series of areas for you to discuss and reflect on with your colleagues. These topics aim to help you assess your firm's position in regard to Cyber Security against international standards. This should not be considered formal guidance or be treated as a list that the Commission will be assessing against but is intended to provide a board range of measures to consider when setting your own Cyber Security frameworks.

Does your firm consider the 5 Pillars of Cyber Security?

- Identification
- Protection
- Detection
- Response
- Recovery

Technical Controls - Does your firm consider the below controls when setting its control framework? Does your firm consider Defence in Depth?

- Vulnerability Management and Patching - patching all security updates rather than just critical and high risk patches
- Penetration Testing and Vulnerability Scanning - ensure weaknesses in your defences are detected before they are used against you
- Network Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS) - have the ability to visualise and detect anomalous events and incidents
- 2 Factor Authentication (2FA)/Multi Factor Authentication (MFA) - all accounts accessed over the untrusted internet should use something you KNOW (username and password) along with something you HAVE (a token, or code sent via SMS), or something you ARE (biometric such as fingerprint, iris or face scan)
- Strong Passwords.
- Email protection tools, especially around phishing
- Antivirus/Antimalware
- Backups - Online and offline and test restoring from backups
- Mobile Device Management (MDM)
- Data Loss Prevention (DLP)

People Controls Training programs - Does your firm consider the following when creating its standard training program?

- Email Scams, Phishing and Social Engineering
- Passwords
- Clear Desk Policy
- Bring-Your-Own-Device (BYOD) Policy
- Data Management
- Removable Media
- Safe Internet Habits
- Physical Security and Environmental Controls
- Malware
- Hoaxes
- What to do when something goes wrong

Core Concepts of Information Security

- Confidentiality– the protection of IT assets and data from unauthorised users.
- Integrity– ensuring that data is accurate, able to be relied upon and has not been changed or modified in an unauthorised manner.
- Availability– ensuring IT assets, data and networks are available to authorised users when they need it to be

Policies, Governance and Controls - Does your firm have policies, procedures and controls that cover the following areas? (these can exist in a single or multiple documents)

- Acceptable Use Policy
- Confidential Data Policy
- Email Policy
- Mobile Device Policy
- Incident Response Policy
- Network Security Policy
- Password Policy
- Physical Security Policy
- Wireless Network and Guest Access Policy

Board Oversight - Does your firm consider the appropriateness of providing the following when creating its management information for its Board.

Current Cyber Security Risks

• Patching/vulnerability status – details of vulnerabilities not patched across the estate, aged by criticality, i.e. criticals/highs/mediums/lows unpatched over 30, 60, 90, 180, 365 days, etc., with reasons why patches not applied or detail what mitigating controls exist
• List any unsupported operating systems/software, roadmaps to migrate to supported versions or timeline to decommission
• Staff education and awareness updates - how many staff are still to complete mandatory annual security training
• Phishing simulation click rates
• Findings of the most recent penetration test, when findings will be mitigated
• Third Party Management

Emerging Risks, Threats and Vulnerabilities:

• What is happening in terms of emerging risks, threat and vulnerabilities, top stories from open source or other threat intelligence feeds/etc.

Incidents

• Numbers of actual events (with analysis on why, did tools work/not work, whether this is a wider risk, what actions are required, lessons learned, etc.)
• Significant near miss events
• Actual breaches
• Data loss events
• Phishing attacks blocked

Compliance Status

• How compliant is the firm with any regulatory requirements, standards and any models or accreditations with which it is aligned, either locally or as part of a group entity.

Useful links

www.ncsc.gov.uk/collection/10-steps-to-cyber-security

www.ncsc.gov.uk/collection/board-toolkit

www.nist.gov/cyberframework/online-learning/five-functions