CYBER FACT SHEET

Multi-factor authentication (MFA),

A strong password can only get you so far - Everyone can enable multi-factor authentication (MFA), but many are not taking advantage of this extra layer of security.

Malicious cyber actors are becoming more sophisticated. Protect your accounts with multi-factor authentication, or MFA.

MFA is a layered approach to securing your accounts online.

When you enable MFA in your online services (like email, bank accounts, etc.), you enter a password like your normally would. Still, you must also provide an authenticator (like a text to your phone, email, face recognition, or other forms) to verify your identity before the service grants you access. If your password becomes compromised, bad actors won't be able to gain access to your accounts because they can't match the second authenticator.

Despite concerns about biometrics [facial, thumbprints etc.] being personal data, the development of new devices will gradually blur the concerns, which may become the new security standard.

Small Firms

Small firms may not consider themselves targets for cyberattacks due to their small size or the perception that they have nothing worth stealing. However, small businesses have valuable information cyber criminals seek, such as employee and customer records, bank account information and access to the business's finances, and access to larger networks. In some ways, small businesses are at a higher risk of cyberattacks than larger businesses because they often have fewer resources dedicated to cybersecurity.

Role of the Principal partner or director

Cybersecurity is about culture as much as it is about technology. The IT team alone are NOT responsible for security.
Culture cannot be delegated. The partner/director is responsible for the following tasks:

1. **Establish a culture of security.** Discuss cybersecurity with all staff. Include cybersecurity in regular email communications to staff. Inform everyone of updates on security program initiatives.

   Include meaningful security objectives aligned with the leadership team's business goals. Security must be an "everyday" activity, not an occasional one.

   Regular back-ups and system updates should be automatic, and staff should be unable to disable the auto-update [server software must be fully patched].

2. **Identify and appoint a "Security Program Manager."** This person doesn't need to be a security expert or IT professional. The Security Program Manager ensures your firm implements all the key elements of a strong cybersecurity program. The manager should report on progress and barriers to you and other senior staff at least monthly.

3. **Review and approve the Incident Response Plan (IRP).** The Security Program Manager will create a written IRP for the leadership team to review. The IRP is your action plan before, during, and after a security incident. Give it the attention, and involve leaders from all Teams, not just IT staff.
   Invoke the IRP even when you suspect a false alarm.
4. **Participate in** tabletop exercise drills.[1] The Security Program Manager will host regular attack simulation exercises called tabletop exercises. These exercises will help the team build the reflexes that you'll need during an incident. Ensure your senior staff attend and participates.
5. **Support the IT team.** Support by the Principal/director is critical, and the help of every staff member is important. Take ownership of certain efforts. Make the MFA announcement to the staff and keep track of the progress. Personally, follow up with people who have not enabled MFA. The culture of security from the top is essential.

Role of the Security Program Manager

The Security Program Manager will need to drive the elements of the security program, inform the partner of progress and barriers, and make recommendations.

These are the Security Program Manager's most important tasks:

1. **Training.** All staff must be formally trained to understand the firm's commitment to security, what tasks they need to perform (like enabling MFA, updating their software and **avoiding clicking on suspicious links that could be phishing[2] attacks**), and how to escalate suspicious activity.
2. Write and maintain the Incident Response Plan **(IRP).** The IRP will spell out the response/s or actions before, during, and after an actual or potential security incident. It will include roles and responsibilities for all major activities and an address book should the network be down during an incident. See the sample Incident Response Plan - advice on what to do before, during and after an incident.
3. **Host quarterly tabletop exercises**
4. **Ensure MFA compliance.** Everyone must use MFA to log into ICT systems, including remote access via laptops, phones etc. A team must review the MFA status regularly.

The Role of ICT

The tasks for the ICT lead and staff include the following:

1. **Ensure MFA is mandated using technical controls. , There must be no exceptions.**
   To regularly look for non-compliant accounts and remediate them. Verify MFA stats.
2. **Enable MFA for all system administrator accounts.** System administrators are key targets for attackers. The Active Directory for global administrators must comply with and use MFA.

---

[1] Teams can conduct exercises to test how to recover from an attack. Partners can initiate discussions about their ability to address a variety of threat scenarios.

[2] The fraudulent practice of sending emails or other messages purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card and bank details.

3. **Patch**. Many attacks succeeded because the victims ran vulnerable software when a newer, safer version was available. Keeping your systems patched is one of the most cost-effective practices to improve your security posture. Where possible, always enable auto-update mechanisms.
4. **Perform and test backups.** Many organisations that have fallen victim to ransomware had no backups or incomplete/damaged backups. It is important to test partial and full restores regularly. There must be a plan for the restoration. Time delays in restoring data or systems impact their business.
5. **Remove administrator privileges from user laptops.** A common attack vector is to trick users into running malicious software. The attacker's job is made easy when users have administrator privileges. A user without administrator privileges cannot install software, and this attack won't work.
6. **Enable disk encryption for laptops.** Modern smartphones encrypt their local storage, as do Chromebooks. Windows and Mac laptops, however, must be configured to encrypt their drives. Protecting your laptop fleet is important, given how many laptops are lost or stolen yearly.

There are, of course, many other IT tasks that add to a good security program. While this list is not exhaustive, it contains the top actions to address the most common attacks.

Achieving the Highest Security Posture

When security experts give cybersecurity advice, they assume you are only willing to make small changes to your IT infrastructure. Some organisations have made more aggressive changes to their IT systems to reduce their "attack surface." For the possibility of falling victim to phishing attacks.

On premise vs cloud

One major improvement you can make is eliminating all services hosted in your offices. These services are known as "on-premise/onsite" services. Examples include servers hosting e-mail, financial systems, databases and applications, and file storage in your office space. These systems require a great deal of skill to secure. They also require time to patch, monitor, and respond to potential security events. Few small businesses have the time and expertise to keep them secure.

While it's not possible to categorically state that "the cloud is more secure," it is repeatedly noticeable that organisations of all sizes cannot continuously handle the security and time commitments of running onsite email, business applications and file storage services. The solution is to migrate those services to secure cloud versions, such as Google Workspace or Microsoft 365, for enterprise email. These services are built and maintained using world-class engineering and security talent at an attractive price. Where possible, firms with onsite systems should migrate to secure cloud-based alternatives as soon as possible.

Secure endpoints

While all operating system vendors work to improve the security of their products continuously, there are no absolute cyber-free products or services. Systems are most vulnerable at their endpoints, i.e., where users connect to the system.

Endpoints represent key vulnerable points of entry for cybercriminals. Endpoints are where attackers execute code and exploit vulnerabilities, as well as where there are assets to be encrypted

or leveraged. With workforces becoming more mobile and users connecting to internal resources from off-premises endpoints worldwide, endpoints are increasingly susceptible to cyberattacks. Objectives for targeting endpoints include, but are not limited to:

- Use an endpoint as an entry and exit point to access high-value assets and information on an organisation's network.
- Access assets on the endpoint to exfiltrate [steal information] or hold hostage, either for ransom or purely for disruption.
- Take control of the device and use it in a botnet to execute a DoS attack.

Managed Service Providers [MSP]

Third-party vendors such as MSPs offer services that can reduce costs and play a critical role in supporting efficient IT operations for organisations of all sizes. Many firms and other small and medium entities use MSPs to manage IT systems, data, and applications remotely. It must be noted that outsourcing the management of networks, cloud infrastructure, applications, devices, and other IT elements to MSPs does not absolve an organisation from risk management responsibilities associated with the IT enterprise.

Key responsible individuals should consider the security practices in place across their firms to answer the following:

- Who is responsible for security and operations when outsourcing ICT services to an MSP?
- What are the most critical assets we must protect, and how do we protect them?
- What should an MSP provide to the firm before a contract award to demonstrate security controls in place?
- What network and system access levels are appropriate for third-party service providers?
- Ensure a risk assessment of MSP is developed and agreed to by the MSP [there are standard benchmarks available that can be used to develop a specific risk assessment for the firm].