# How Organisations and Their Employees Can Stay Ahead of Cybersecurity Threats

As organisations continue to rely heavily on technology and digital infrastructure, cybersecurity has become a critical aspect of operations to protect customers' data and ensure business continuity. Organisations are encouraged to protect sensitive data, ensure the integrity of their systems, and take proactive measures to safeguard against any cybersecurity threats.

Employees play an important role in organisations' cybersecurity as they are the first line of defences against potential threats and cybersecurity awareness. Organisations are encouraged to raise their employees' cybersecurity awareness by conducting incident response simulation exercises and highlighting the importance of identifying and reporting any phishing attempts. Organisations can consider implementing robust password management and bring-your-own devices policies to protect themselves from unauthorised access and data loss. Additionally, organisations should develop clear guidelines on cyber incident reporting.

The purpose of this advisory is to provide a reference guide for organisations' IT departments and cybersecurity professionals on how they can stay ahead of cybersecurity threats. It covers the following topics:

- Conduct Incident Response Simulation Exercises
- Define and Review Incident Reporting Procedures
- Raise Awareness of the Dangers of Phishing Attacks
- Establish and Enforce Password Policies
- Incorporate Cybersecurity Measures in Bring Your Own Device (BYOD) Policy

**Conduct Incident Response Simulation Exercises**

Organisations and their incident response teams can benefit from simulation exercises as these exercises provide verification on whether the organisation's response strategy is effective and highlight any weaknesses that require immediate attention. Such exercises also allow internal stakeholders to be familiar with procedures to improve response and recovery efficiency when an actual incident occurs.

These are the following steps that organisations may consider taking when conducting incident response simulation exercises:

Detailed and Clearly Defined Plan

The objectives of the simulation exercises must be defined clearly to meet the expected outcomes e.g. fostering inter-department collaboration and coordination, which could result in better preparedness during a cyber incident. Having a well-organised plan would allow participants to be aware of their respective roles and responsibilities during a cyber incident.

Creation of Realistic Scenarios

Scenarios should be realistic to simulate potential cyber-attacks that could be detrimental to the organisation's security posture. These scenarios require participants to be creative and think of a workaround to circumvent these constraints. Various challenges like resolving the given scenarios under the stipulated time and introducing technical constraints during the exercise play can be implemented.

Comprehensive Testing

Thorough testing of the devised plan should be conducted to evaluate its effectiveness and efficiency. Such tests include stress tests that can be performed on tools and networks to determine how well they can perform under pressure. The results of the test can be documented for future improvement on current processes.

Post-Exercise Debrief

Post-exercise debriefs can be conducted after the simulation exercises to seek feedback from participants. This helps to identify areas for improvement and flag any ineffectiveness in the plan so that the existing incident response plan can be further improved.

Regularly Update the Incident Response Plan

It is imperative to regularly update the incident response (IR) plan and ensure that it is up-to-date. The following are areas(non-exhaustive) which organisations could monitor and review for updates periodically:

- Security requirements
- Technical requirements
- Contact maintenance
- External contact maintenance
- Significant changes in hardware or software appliance

Proper documentation should be in place to ensure that any changes in the IR plan can be tracked. Copies of the approved IR plan can be made available physically or electronically to allow employees to access to different forms of the IR plan.

There are various types of incident response simulation exercises that organisations could consider:

Tabletop Exercises

Tabletop exercises allow participants to go through recovery operations procedures in a simulated environment and could be held multiple times a year. These exercises may be discussion-based and require participants to work as a group.

Functional Exercises

Functional exercises require key personnel to validate plans and readiness by performing their duties in a simulated environment. Held annually, operations-based functional exercises are more extensive and realistic compared to tabletop exercises which require a simulated environment. Scripts are usually provided for personnel to perform role-playing of entities such as the incident response team.

Full-Scale Exercises

Operations-based full-scale exercises may allow organisations to better gauge their resource utilisation when an incident occurs. However, such exercises might utilise most of the organisation's resources, which can be disruptive to the organisation's operations. As such, these exercises are only held once every few years.

**Define and Review Incident Reporting Procedures**

Incident reporting procedures play a vital role in maintaining a secure digital environment within the organisation. Timely and accurate reporting of cyber incidents enables organisations to respond quickly and implement the necessary mitigation measures, which minimises the impact of the incident. By defining incident reporting procedures clearly, organisations are encouraging their

employees to be more aware of the cybersecurity threats that they may encounter and how they can report cyber incidents efficiently and effectively. As cybersecurity threats are constantly evolving, it is important for organisations to review their incident reporting procedures regularly to ensure that their employees' cyber incident response capabilities remain up to date.

The following (non-exhaustive) are best practices that organisations may consider implementing to raise awareness on incident reporting procedures established by the organisation:

Establish and Promulgate Incident Reporting Channels

Establish clear and easily accessible reporting channels for cyber incidents which may include a dedicated email address or phone number of the IT or cybersecurity team responsible for incident response.

Develop Incident Reporting Templates

Develop incident reporting templates to guide employees in providing the necessary information pertaining to cyber incidents. Such information may include the date, time, description of the incident and any relevant evidence. Organisations may also consider creating detailed guidelines on the process of reporting a cyber incident to ensure the accuracy of the information provided.

Establish Incident Response Team

Designate an incident response team comprising individuals with specific roles and responsibilities. Organisations should ensure that the incident response team has the necessary expertise and resources to handle the reported cyber incidents efficiently and effectively. To ensure that the incident response team continues to be updated with the evolving threats, organisations are encouraged to provide them with training and regular exercises.

Regularly Review Incident Reporting Procedures

Regularly review and update incident reporting procedures based on lessons learnt from previous cyber incidents or simulation exercises. Organisations may also consider collecting feedback from their employees to identify any challenges or bottlenecks in the reporting process.

**Raise Awareness of the Dangers of Phishing Attacks**

Phishing is the most common form of cybercrime where sensitive information may be stolen through various forms of electronic communication such as emails and text messages. As phishing attacks may target anyone in the organisation, it is essential for organisations to raise awareness of the various type of phishing attacks among their employees.

Organisations can consider undertaking the following measures/initiatives to raise awareness amongst employees on the dangers of phishing and how to avoid falling victim to phishing attacks:

Employee Training

Organisations can implement regular training to educate employees about the different types of phishing attacks, common phishing techniques and how to identify and respond to suspicious emails, links, and attachments. As phishing techniques are constantly evolving, organisations are encouraged to review their training materials and ensure that employees are up to date with the current phishing techniques. Organisations may also consider conducting organisation-wide security awareness campaigns to reinforce the importance of cybersecurity practices covered during the training.

Phishing Attack Simulations

Phishing attack simulations may be leveraged to test and reinforce knowledge gained from the training sessions. A reputable phishing simulation tool should be used to create realistic scenarios and measure employees' responses. Such a tool can detect when and which employee has clicked on the phishing link or opened the attachment. Through these simulations, organisations can identify employees who may be more vulnerable to phishing attacks and educate them on the possible risks of such attacks. Additionally, organisations can provide further guidance on how employees can improve their phishing detection skills.

**Establish and Enforce Password Policies**

Passwords are the first line of defence against any unauthorised access to organisation accounts. By implementing robust password policies, organisations can strengthen their cybersecurity posture and ensure that cybercriminals cannot easily access their confidential data. Hence, organisations are advised to establish and enforce best practices in password management policy for employees to follow and to manage passwords securely.

Organisations are advised to consider the following requirements in a password policy:

Password Complexity Requirements

The use of strong passwords that are complex, unique, difficult to guess and hard to crack should be enforced for organisational accounts. Password complexity requirements should include at least 12 characters comprising upper-case and lower-case letters, numbers and special characters. To help employees remember their passwords, organisations may encourage them to use passphrases by putting together a sentence or combination of words based on a memory unique to them. Passphrases are more secure than typical passwords as they are generally longer and require significantly more time for cybercriminals to crack. Employees can find out the strength of their password here.

Enforce Password History Policy

Enforcing password history policy encourages employees to use a new password that differs from their previous passwords, preventing any old or compromised passwords from being reused. By regularly refreshing passwords and maintaining a password history, the organisation would significantly reduce the risk of unauthorised access to their employees' accounts.

Implement Multi-Factor Authentication (MFA)

Enable MFA for employees' accounts, whenever possible, as they provide an additional layer of security for the employees' online accounts. It requires two or more verification factors before access is granted to their applications or online accounts.

There are three main types of authentication methods that MFA is based on:

- Things you **know** (knowledge) such as password or pin;
- Things you **have** (possession) such as one-time passwords (OTPs) from physical OTP tokens or smartphones;
- Things you **are** (inherence) such as biometrics involving fingerprints or voice/facial recognition

Reduce Password Expiration Frequency

Enforcing mandatory password expiration may diminish the effectiveness of the password expiration practice as employees may resort to replacing their passwords with slight variations of their previous passwords. To prevent this, organisations are encouraged to enforce password expiration only when there is evidence of an employee's account password being compromised.

**Incorporate Cybersecurity Measures in Bring Your Own Device (BYOD) Policy**

BYOD policy allows employees to use their personal devices for work-related purposes, providing flexibility and convenience. However, this could potentially lead to an increase in cybersecurity risks when not properly managed as employees may not have adequate security measures on their personal devices or are unaware of potential cybersecurity threats that they may encounter. As a result, organisations are advised to establish and enforce cybersecurity measures in their BYOD policy to safeguard employees' personal devices and organisations' data from cybersecurity threats.

The following (non-exhaustive) are best practices that organisations may consider implementing to raise awareness of cybersecurity regarding BYOD policy:

Comprehensive Acceptable Use Policy

An acceptable use policy (AUP) is a document stipulating constraints and practices that an employee must agree to before accessing the corporate network or resources. A comprehensive AUP should contain the organisation's data management policies to protect the organisation against data loss and ensure security on all devices connected to the organisation's data system should an employee's personal account be compromised. Such policies should clearly state the responsibilities and expectations of the employees when using their personal devices for work-related purposes. Additionally, organisations should advise their employees against storing any organisation credentials in their personal accounts.

Regularly Update Software and Operating Systems

Organisations should mandate that their employees update their devices' software and operating systems with the latest security patches. This helps to reduce the risk of unpatched vulnerabilities being exploited. Organisations should also encourage employees to enable automatic updates, where available, and provide clear guidelines on how to configure their devices to receive such updates.

Ensure Secure Network Communications

The use of Virtual Private Network (VPN) to encrypt the connections between an employee's personal devices and the organisation's network should be enforced. This provides a layer of security to protect sensitive information from unauthorised access or interception. Organisations should also encourage employees to connect to secure and trusted Wi-Fi networks when accessing company resources.

Enforce Password Requirements

Password requirements for all employees' devices used for work-related purposes should be enforced to prevent any unauthorised access. Organisations are also advised to implement a password management policy for employees to follow and manage passwords securely.

Raise Awareness Amongst Employees on the BYOD Policy

Organisations should raise awareness amongst their employees on their BYOD policy, the risks involved and the cybersecurity measures regarding the policy before allowing them to use their personal devices for work-related purposes. Additionally, employees should be trained to identify and report suspicious activities on their personal devices based on clear guidelines set by the organisation.

**Do not make it easy for cybercriminals.** Cybersecurity is a shared responsibility and by implementing robust cybersecurity best practices, organisations can significantly enhance their overall security posture. With the best practices in place, organisations and their employees are

empowered to proactively identify and respond to cyber incidents, strengthen their defence against evolving threats, and protect sensitive data and resources from unauthorised access.

**References:**


https://techcult.com/most-common-passwords/
https://www.onelogin.com/learn/what-is-mfa
https://www.ncsc.gov.uk/blog-post/problems-forcing-regular-password-expiry
https://www.cmu.edu/iso/governance/guidelines/password-management.html
https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
https://heimdalsecurity.com/blog/byod-bring-your-own-device/
https://www.ready.gov/exercises
https://ncsc.gov.uk/guidance/phishing
https://cloudstrike.com/cybersecurity-101/phishing/phishing-attack-awareness-training/