ADVISORY ON CYBERSECURITY FOR GENERAL ELECTIONS 2025 FOR POLITICAL PARTIES AND CANDIDATES

1. Introduction

In today's digitally interconnected world, the integrity of election processes is increasingly challenged by cyber threats. Political parties, candidates, and their teams are often the target of sophisticated cyber-attacks aimed at disrupting services, stealing sensitive data, and spreading misinformation. These attacks can undermine public confidence in the electoral process, hinder campaign efforts, and tarnish reputations. To navigate this complex landscape, it is crucial for all stakeholders —including candidates, political parties, and election officials —to be aware and stay vigilant of potential cyber risks, particularly those enabled by emerging technologies such as advanced artificial intelligence (AI).

This advisory outlines the potential key cyber threats and provides preventive measures that election candidates and political parties in Singapore can take to reduce the risk of cyber incidents disrupting their operations.

2. Potential Cyber Threats

Five general categories of threats were observed during elections conducted in other countries. They are (i) Disruption of Services, (ii) Data Theft and Breaches, (iii) Manipulation and Misinformation, (iv) Insider Threats, and (v) Social Engineering.

2.1. Disruption of Services

Disruption of services during election campaigns can severely hinder communication, outreach, and overall operations. Such disruptions can affect websites, data accessibility, and general network functionality. They may take the following three forms:

2.1.1. Distributed Denial of Service (DDoS)

A DDoS attack is a malicious attempt to disrupt the normal traffic of a website, server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of traffic that could exhaust the capacity of the web resource to handle multiple requests or connections.

A DDoS attack could result in the unavailability of a political party’s websites or network services, denying members of the public from accessing them. A threat actor can use AI to

analyse the optimal times and methods for their attack to evade detection and bypass traditional security defences. This can affect a political party's or candidate's campaign efforts. A threat actor may also use DDoS as a distraction while infiltrating the network to compromise sensitive data which may subsequently be leaked onto the Internet.

2.1.2. Ransomware

Ransomware is a malware designed to encrypt files stored in a compromised system until a ransom is paid. The malware renders all affected files irrecoverable unless a decryption key is available. Some ransomware variants are known to traverse across the network and encrypt all files stored in shared or network drives, including backups stored on the same compromised network. There is no guarantee that victims will get the decryption key or recover their data even after the ransom is paid. The inability to access these encrypted files could affect a political party's or candidate's campaign efforts.

A ransomware attack is typically carried out via phishing emails that contain malicious attachments or links. Users' systems can get infected when they click on these attachments or links. It can also occur when unsuspecting victims unknowingly visit an infected website that downloads and installs the malware onto their devices. Some threat actors may use AI to identify vulnerable targets and customise attacks to exploit specific vulnerabilities in the users' systems. AI can also be used to enhance the malware's ability to evade detection, increasing the likelihood of a successful and well-timed attack.

2.1.3. Website Defacement

Website defacement happens when a threat actor gains unauthorised access to an official website and changes its visual appearance. These changes often involve modifying or replacing web pages like home pages or sub-pages. A threat actor can make a website inaccessible by removing all content. The defaced site may display misleading or false information, defamatory content, disturbing images, or inappropriate messages, potentially damaging the credibility or reputation of the party or candidate.

2.2. Data Theft / Breaches

Data theft is stealing information from a computer system, database server, email account, or any device that stores digital information. Threat actors can leverage many possible attack vectors, such as social engineering, planting malware, and infiltrating computer networks or security systems. Many of these means of entry into the system are gained through phishing emails.

A threat actor may also attempt to gain unauthorised access to critical infrastructure through various means, including exploiting vulnerabilities or using stolen credentials. The threat actor can automate the discovery and exploitation of vulnerabilities using AI, making attacks quicker and more efficient. This can result in the manipulation or deletion of data, exposure of sensitive information, and disruption of election processes.

The threat actor can publish or sell the stolen data, resulting in reputational damage to the party or candidate. The threat actor can also use AI to analyse large volumes of stolen data to quickly extract valuable information for targeted misinformation campaigns. The stolen data can also be used to launch further attacks on other related information technology (IT) systems.

2.3. Manipulation, Misinformation and Disinformation

Manipulation, misinformation or disinformation can significantly impact the integrity and fairness of elections. Manipulation refers to unauthorised changes to official documents often done by controlling official accounts of the candidates or parties. Misinformation is the publication of inaccurate information stemming from mistakes or misunderstandings without the intent to deceive. Disinformation is the intentional spread of falsified information to deceive or harm political parties and candidates. These actions may mislead voters, compromise official candidate accounts, damage reputations and influence election outcomes. Manipulation, misinformation and disinformation may take the following forms:

2.3.1. Compromised/Fake Social Media Accounts

Threat actors can compromise social media accounts belonging to election candidates or political parties to spread false or misleading information. These compromised accounts can be used to launch phishing attacks, tricking users into revealing sensitive information such as login credentials or personal data. Additionally, fake or impersonation accounts mimicking legitimate candidates or parties may be created on various social media platforms for the same purpose. These fake accounts can be used to conduct financial scams such as soliciting donations for fake causes. Attackers could use these fake social media accounts to post AI-generated content that could damage reputations and influence election outcomes. Candidates are advised to verify their social media accounts whenever possible.

2.3.2. Scams

Threat actors could use the context of General Elections to conduct financial related scams. This can come in the form of soliciting donations for fake causes, impersonating candidates to promote a fake product to their supporters or impersonating the Elections Department to lead the victim to a scam website.

The use of AI has also been used in scams to write messages, create images/videos/voice recordings to enhance the credibility of their scam. It can also be used to analyse the victim's background to create a targeted scam that aligns with their political beliefs. The manipulation from threat actors can cause reputational damage to the candidate or party and financial loss for the voters as well.

2.3.3. Deepfakes and Disinformation/Misinformation

Deepfakes refer to multimedia (images, videos, and audio) that are synthetically created or manipulated. They can be used to convincingly depict election candidates saying or doing things they never did. These fake AI-generated content produced by threat actors are designed to quickly go viral through re-publication of misinformation (by unsuspecting readers) or through disinformation campaigns, reaching a broad audience and impacting public perception, possibly damaging the credibility or reputation of the party or candidate.

2.4. Insider Threats

Insider threats refer to threats from someone inside the organisation who has authorised access to a system or network. He/she may wittingly or unwittingly use such access to harm the network. A malicious insider within an election campaign may intentionally leak or steal sensitive information or compromise network security, allowing external sources unauthorised access to critical systems. Data that may be exfiltrated as a result could damage the reputation of the party or candidate.

2.5. Social Engineering

Social engineering is a manipulation technique that exploits human weaknesses to attain information, gain access, or achieve monetary gains. Social engineering attacks may take the following forms:

2.5.1. Phishing

Phishing is a social engineering tactic designed to trick individuals into divulging sensitive information, such as login credentials or financial information. Threat actors may impersonate a trustworthy entity such as a political party to trick victims into clicking on a link or an attachment that could allow malicious malware to download to the system. The phishing links then lead to fraudulent websites luring victims to reveal personal or confidential information. Threat actors have, in recent years, used AI to craft highly personalised and convincing phishing emails or messages, increasing the likelihood of a successful attack. These phishing campaigns can be automated and scaled up while continuously adapting tactics based on real-time feedback and response patterns.

2.5.2. Vishing

Vishing is a form of voice phishing involving phone calls to impersonate trusted entities, such as government officials, technical support, or election officials. With AI, threat actors can create realistic voice clones of these trusted individuals that can be used in phone calls to deceive targets into extracting sensitive information, convincing individuals to reveal their credentials, or installing malware.

3. Precautionary Measures for Election Candidates and Political Parties

Various IT equipment and systems may be used to support election candidates or political parties' campaigns. Such technologies may introduce potential cyber threats, highlighted in the previous section. Election candidates and political parties need to be responsible for their cybersecurity and are advised to take precautionary measures to safeguard their digital assets.

Election candidates and political parties should appoint an experienced person to take charge of their campaign's cybersecurity matters. Due consideration should also be placed on engaging a cybersecurity vendor to review and manage the cybersecurity posture of the election campaign systems and respond to any cybersecurity incident. Below are some precautionary measures that election candidates and political parties can implement to safeguard cybersecurity. Please note that the measures provided are not exhaustive.

3.1. Establish a Complete Inventory of Digital Assets and Implement Strict Access Control

- Perform a stocktake of all digital assets owned and used by the election campaign. For example, a clear understanding of what, where, and how data is stored on each device.
- Institute strict control over administrator and remote access privileges to digital assets. The principle of least privileges should be followed as much as possible - users and devices should be given the minimum permissions required to perform their assigned tasks and responsibilities.
- Establish a whitelist of applications (apps) that are allowed to run on device(s) used for campaign purposes, especially those containing or processing sensitive data. All other apps should be disallowed.

3.2. Plan for Resiliency of Operations

- Ensure systems can continue operations by implementing redundancy and high availability measures to resist DDoS attacks. This can be achieved using secondary systems that will fail-over from the primary system if it is inaccessible. Use of load balancers can also ensure traffic is distributed efficiently.
- Perform regular backup and test the ability to restore from those backups to lessen the impact of ransomware or defacement attacks.
- Establish a secure secondary communication channel to ensure there is another platform for effective communication.
- Ensure any changes (e.g. patching, configuration changes, etc.) to critical systems are tested before deployment to production.

3.3 Enforce Strong Authentication Controls for all Campaign Accounts

- Institute strong passwords that are complex, unique, difficult to guess for campaign and campaign-related accounts, containing at least 12 characters comprising upper-case and lower-case letters, numbers, and/or special characters.
- To make it easier for you to remember, you can use passphrases by putting together a sentence of combination of words based on a memory unique to you. As passphrases are longer than traditional passwords, they are more secure as it often requires significantly more time for cybercriminals to crack than short passwords.
- Implement multi-factor authentication (MFA) to secure all accounts, including email, social media, and internal platforms, and securely store backup codes and methods.

- MFA is a security control measure that requires users to provide two or more factors of identification before access is granted. This layered approach ensures that even if one factor, like a password, is compromised, additional verification factors are needed before attackers can compromise the account. The factors used in MFA are typically categorized as follows: Knowledge Factor (Passwords or Passphrases), Possession Factor (Passkeys and Fast Identity Online (FIDO)), Inherence Factor (Biometric data), Location-based Factor (Current location), Behaviour-based Factor (Pattern recognition or behavioural biometrics used to create a baseline profile to recognise anomalous behaviour).
- As an alternative to password/passphrase-based authentication, Passkeys and FIDO are also gaining adoption for being able to provide more secure and user-friendly authentication through the use of public-private keys. The private key is securely stored on your device (e.g., smartphone, computer) while the public key is stored on the service's server. As the private key never leaves your device, it cannot be intercepted by attackers.
- Raise awareness amongst account holders on safeguarding account credentials (e.g. do not share the credentials with anyone and do not write the password down on paper).

3.4 Perform Regular Software Updates

- Periodically scan all campaign-related systems and devices for known vulnerabilities and update them regularly by promptly applying the latest security patches. If immediate patching is not possible or feasible, vendor-provided mitigations should be implemented. Set automatic updates where feasible.

3.5 Regularly Back Up Important Data

- Schedule regular backups of all critical data to ensure data integrity and availability in the event of a cybersecurity incident such as ransomware. Backups should be encrypted and stored in multiple locations, including offsite and cloud-based solutions, to prevent threat actors from compromising the primary and backup systems in the same attack. In addition, the backups should be regularly tested to ensure that the backup data can be recovered and restored in time to recover from data corruption or destruction.

3.6 Raise Cybersecurity Awareness and Adoption Amongst Campaign Staff and Volunteers

- Conduct regular security awareness training to educate campaign staff and volunteers on common cybersecurity threats. Regularly remind them to be alert to phishing and other social engineering tactics and implement preventive measures.
- Establish protocols for verifying information about deepfakes and manipulated content before it is shared or acted upon.
- Establish clear lines of communication for incident reporting. Campaign staff should also be encouraged to report near-miss and/or suspicious incidents.
- Train campaign staff to spot signs of compromise (e.g. the inability to log in using an original password, receiving a ransom message, the sudden presence of unknown applications installed on a device, or inexplicable activities detected on their device). Provide guides, checklists, and other resources to help staff understand and apply best practices.

3.7 Develop Cybersecurity Monitoring and Incident Response Capabilities

- Establish cybersecurity monitoring capabilities to detect breaches or breach attempts. Such capabilities can be in the form of installed technologies such as Endpoint Detection and Response (EDR) and Intrusion Prevention Systems (IPS).
- Perform regular security assessments on election campaign-related websites using reputable tools such as SSL Labs, MxToolbox, or the Cyber Security Agency of Singapore's Internet Hygiene Portal to identify possible flaws for remediation.
- Enable logging of network traffic and security events. Logs should be retained for a suitable period (e.g. 6 months) to facilitate any investigations in the event of a cybersecurity incident.
- Develop a comprehensive incident response and management plan outlining steps to take during various security incidents, ensuring all stakeholders know their roles. The following checklist, developed by SingCERT, may be helpful when developing an incident response plan for your campaign: https://www.csa.gov.sg/resources/singcert/incident-response-checklist.

4. Steps to Take in the Event of a (Suspected) Cybersecurity Incident

If election candidates, political parties, or campaign staff suspect that a cybersecurity incident may have occurred, they should:

- Lodge a police report if you suspect your account(s) or system(s) have been compromised or misused.
- Keep the Elections Department of Singapore (ELD) informed.

To respond to the incident:

- Contact the relevant email and social media platform providers for issues related to your email or social media accounts. For the contact addresses, please refer to the Useful Links for Email Providers and Social Media Platforms.
- If your IT system is compromised, contact your appointed cybersecurity vendor. The section Cybersecurity Service Providers provides a non-exhaustive list of cybersecurity vendors. You should also report it to Singapore Cyber Emergency Response Team (SingCERT) at https://www.csa.gov.sg/cyber-aid.

5. Additional Resources

For additional information on the potential cyber threats mentioned in this advisory and other cybersecurity tips and good practices, please refer to the section Useful References.

For clarifications on the advisory, please email SingCERT at singcert@csa.gov.sg.

6. Useful Links for Email Providers and Social Media Platforms

1. If you encounter issues with your email accounts

Email Provider	Email Contact
Gmail	https://support.google.com/accounts/answer/6294825
Outlook or Hotmail	https://support.microsoft.com/en-hk/help/10494/microsoft-account-how-to-access-a-compromised-account
Yahoo	https://help.yahoo.com/kb/recognize-hacked-yahoo-mail-account-sln2090.html

2. If you encounter issues with your social media accounts

Social Media	Contact Information

Platform	
Facebook/Meta	**Verify Account** https://www.facebook.com/help/1288173394636262 **Compromised Account** https://www.facebook.com/hacked **Impersonation Account** https://www.facebook.com/help/174210519303259/
X	**Verify Account** https://help.x.com/en/managing-your-account/about-x-verified-accounts **Compromised Account** https://help.x.com/en/safety-and-security/x-account-compromised **Impersonation Account** https://help.x.com/en/forms/authenticity/impersonation
Instagram	**Verify Account** https://help.instagram.com/854227311295302 **Compromised Account** https://help.instagram.com/368191326593075 **Impersonation Account** https://help.instagram.com/446663175382270
YouTube	**Verify Account** https://support.google.com/youtube/answer/3046484?hl=en **Compromised Account** https://support.google.com/youtube/answer/76187?hl=en **Impersonation Account**

	https://support.google.com/youtube/answer/2801947?hl=en
LinkedIn	**Compromised Account** https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en **Impersonation Account** https://about.linkedin.com/transparency#profiles
Snapchat	**Verify Account** https://businesshelp.snapchat.com/s/article/public-profile-verify **Compromised Account** https://help.snapchat.com/hc/en-us/articles/7012305621908-My-account-is-compromised **Impersonation Account** https://help.snapchat.com/hc/en-us/requests/new
TikTok	**Verify Account** https://support.tiktok.com/en/using-tiktok/growing-your-audience/how-to-tell-if-an-account-is-verified-on-tiktok **Compromised Account** https://support.tiktok.com/en/log-in-troubleshoot/log-in/my-account-has-been-hacked **Impersonation Account** https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-user

3. If you encounter issues with your messenger accounts

Messaging Platform	**Contact Information**
Telegram	**Verify Account** https://telegram.org/verify

	Compromised Account https://telegram.org/support **Impersonation Account** https://telegram.org/support

7. Cybersecurity Service Providers

Political parties should consider appointing a professional cybersecurity vendor to review and manage the party's cybersecurity posture and deal with any cybersecurity incident. A non-exhaustive list of cybersecurity vendors who are CREST members with a local office in Singapore and provide incident response services is provided for reference. You may also visit this website for more information.
https://www.crestapproved.org/members/?filter_accredited_services_10717=Cyber%20Security%20Incident %20Response&filter_offices_10717=Singapore

S/N	Cybersecurity Service Providers
1	Cisco
2	CrowdStrike
3	Deloitte Touche Tomatsu Ltd
4	F-Secure Consulting
5	KPMG LLP
6	Nettitude Group
7	PricewaterhouseCoopers LLP (PwC)

8	SEC Consult

8. Useful References

For more information on potential cyber threats to your campaign and possible preventive measures you can take to secure your IT systems, please visit the following websites:

Distributed Denial of Service (DDoS)

- https://isomer-user-content.by.gov.sg/36/4b827849-0a11-46d1-8dd1-8c1d883af72f/Playbook-for-DDoS.pdf
- https://isomer-user-content.by.gov.sg/36/19fe1d86-042e-406e-adf5-710947c3374b/infographic-on-mitigating-ddos-attacks.pdf
- https://dg3bna7r99uuk.cloudfront.net/resources/publications/distributed-denial-of-service--ddos--mitigation-advisory/

Ransomware

- https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2021-009/
- https://isomer-user-content.by.gov.sg/36/31599eb6-80ca-44b4-8ed5-8cd3cce83afd/Ransomware-Response-Checklist.pdf
- https://www.police.gov.sg/Advisories/Crime/Cybercrime/Ransomware
- https://www.nomoreransom.org/en/index.html

Website Defacement

- https://www.csa.gov.sg/alerts-and-advisories/advisories/ad-2022-007
- https://www.csa.gov.sg/alerts-advisories/Advisories/2023/ad-2023-021

Data Theft / Breaches

- https://isomer-user-content.by.gov.sg/36/02db9352-fbea-4699-98d2-b6213ed1c0f2/protecting-yourself-from-data-breaches.pdf
- https://isomer-user-content.by.gov.sg/36/08913a84-f490-48f7-a115-9cd03de55a36/protecting-your-organisation-from-data-breaches.pdf

Compromised/Fake Social Media Accounts

- https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely

- https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Social_Media_Account_Protection_508.pdf

Deepfakes/Disinformation Campaigns

- https://www.csa.gov.sg/alerts-advisories/Advisories/2024/ad-2024-006

Insider Threats

- https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats
- https://www.cisa.gov/topics/physical-security/insider-threat-mitigation
- https://www.ncsc.gov.uk/files/Reducing-data-exfiltration-by-malicious-insiders-web.pdf

Phishing / Social Engineering

- https://www.csa.gov.sg/our-programmes/cybersecurity-outreach/cybersecurity-campaigns/the-unseen-enemy-campaign/beware-of-phishing-scams
- https://www.csa.gov.sg/News-Events/Press-Releases/2024/csa-releases-playbooks-for-the-conduct-of-simulated-phishing-exercises-to-encourage-organisations-to-improve-their-cyber-defences

Incident Response

- https://www.csa.gov.sg/resources/singcert/incident-response-checklist/
- https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-response-playbooks
- https://www.csa.gov.sg/Tips-Resource/internet-hygiene-portal

Recommended Security Apps

https://www.csa.gov.sg/resources/tips-and-resources/recommended-security-apps-list