ADVISORY TO POLITICAL PARTIES ON CYBERSECURITY RISKS AND PRECAUTIONARY MEASURES

1. In recent years, there have been reports of threat actors launching cyber-attacks during elections and compromising Information Technology (IT) systems used by political parties and candidates in an attempt to disrupt the election process in various countries. The same may happen during our General Election.

2. Political parties and candidates are responsible for their own cybersecurity, and need to strengthen their cybersecurity posture, and take precautionary measures to protect their assets and online presence. This includes all ***IT infrastructure including any smartphone, computer and computing device, online and social media assets, as well as data storage and management***.

3. This advisory provides information on some of the potential cyber threats and good practices political parties and candidates can take to manage and mitigate the risks. It should be read in conjunction with the advisory on threat of foreign interference in elections and precautionary measures.

Potential Cyber Threats

4. Three general categories of threats were observed during the elections conducted in other countries. These are (1) Website Defacement; (2) Disruption; and (3) Data Theft/Breach.

Website Defacement

5. Website defacement happens when a threat actor gains unauthorised access to an official website to change the visual appearance of the website. It may be done either on the website homepage or on subsequent pages of the website. On the defaced page, a threat actor may post disturbing or graphic images, or leave a message to express a view.

6. Defacements could be used to bring down the website and disrupt the operations of the political party, or it could be used to put out false or misleading information that could affect a political party's or candidate's reputation.

Disruption

7. Disruption may take the following forms:

Distributed Denial of Service (DDoS)

8. A DDoS is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. Such attacks utilise multiple compromised machines including computers and other devices connected to the Internet to exhaust the resources of the target. A DDoS attack could cause a service disruption and deny legitimate users access to the services.

9. A DDoS attack could result in unavailability of websites or network services. This could affect a political party or candidate's campaign efforts.

Ransomware

10. Ransomware is a type of malicious software (malware) designed to hold a victim's files or deny access to a computer system until a ransom is paid. The malware locks down the system or encrypts all the data, rendering them irrecoverable unless a decryption key is available. Some variants of ransomware are known to traverse across the network and encrypt all files that are stored in shared or network drives, including backups that are stored on the same network. There is no guarantee that victims will get the decryption key or recover their data even if the ransom is paid.

11. A ransomware attack is typically carried out via phishing emails containing malicious attachments or links. Users' devices could get infected when they open these malicious attachments or links, or if they install pirated software which masks the ransomware in it. Malicious advertisements could also be used to exploit vulnerabilities in a user's browser to install the ransomware in a victim's device.

<u>Data Theft / Data Breach</u>

12. Data theft is the act of stealing information from a computer system, database server, email account, or any device capable of storing digital information. There are many possible vectors of attack for threat actors to carry out, such as social engineering, unauthorised access to systems, planting malware and infiltrating computer network or security systems. Many of these means of entry to the system may be done through a phishing email.

13. A threat actor could publish or sell the stolen data which could result in reputational damage. A threat actor could also utilise the stolen data to launch more attacks on other information technology (IT) systems, if account numbers and passwords were involved.

Phishing

14. Phishing is a form of social engineering tactic to gain access into a system or to entice a user to provide sensitive information. Threat actors may impersonate a trustworthy entity to trick victims into clicking on a link or an attachment that could allow malicious malware to download to the system. Some phishing links also lead to fraudulent websites that lure victims to reveal personal or confidential information, or to proceed with payment for fraudulent transactions.

15. Threat actors may conduct phishing attempts to obtain sensitive party information, or gain access to the system to disrupt the electoral process.

Precautionary Measures

16. Political parties and candidates use various IT infrastructure to support their election campaigns and are responsible for their own cybersecurity. They need to be mindful of the potential cyber threats related to the use of the IT infrastructure, and take precautionary measures to safeguard all their IT infrastructure.

Political Parties

17. Political parties should appoint someone to take charge of their political party's cybersecurity matters. Political parties should also consider appointing a professional cybersecurity vendor to review and manage the cybersecurity posture for their party, as well as to deal with any cybersecurity incident. The areas of review include, but is not limited, to the following:

Access Control

- Know your digital assets/data - what, where and how data is stored, and make sure that important data are encrypted and backed-up;
- Allow only authorised software to run on networks/systems;
- Control or restrict administrator and remote access privileges, especially when systems are outsourced to vendors; and
- Ensure authorised access to networks or systems, and implement Multi-Factor Authentication, where possible.

Timely Control

- Check and patch any network and systems vulnerabilities in the IT infrastructure promptly

Cybersecurity Monitoring and Incident Response

- Establish cybersecurity monitoring capabilities to detect breaches;
- Enable security loggings, if available; and
- Establish and validate an incident response and management plan.

Candidates

18. At the individual level, candidates and members of the campaign team should practice good cyber hygiene, such as:

- Keeping devices' software updated;
- Installing anti-virus protection and firewall;
- Using strong password, and two-factor authentication for devices and social media accounts where possible;
- Back up data on your devices regularly;
- Be vigilant for phishing emails or text messages; and
- Monitor for unusual activities in your devices or accounts.

19. If political parties and candidates suspect their account(s) or system(s) have been compromised or misused, they should lodge a Police report immediately, and also keep the Elections Department informed.

20. To resolve the issue:

- Contact the relevant online platform service providers directly for issues related to your email, social media or web conferencing accounts. A list of the contacts for these providers is available at "**Contacts for Online Platform Service Providers**".
- Contact your appointed cybersecurity vendor if there is any issue with your IT infrastructure. A non-exhaustive list of cybersecurity vendors is provided at "**Cybersecurity Service Providers**".

Additional Resources

21. For cybersecurity tips and good practices, visit https://www.csa.gov.sg/gosafeonline and https://www.csa.gov.sg/singcert.

22. For any clarifications on the advisory, you can email SingCERT at enquiry@csa.gov.sg.

CYBER SECURITY AGENCY OF SINGAPORE
ELECTIONS DEPARTMENT
20 APRIL 2020

Contacts for Online Platform Service Providers

Service Provider	Contact Information
Cisco WebEx	**Live Streaming Issues** https://help.webex.com/contact **Support Hotline** **Toll Free**: 1 800 6221034 **Singapore**: +65 6317 5554
Facebook	**Compromised Account** https://www.facebook.com/hacked **Impersonation Account** https://www.facebook.com/help/174210519303259/ **Live Streaming Issues** https://www.facebook.com/help/587160588142067
Gmail	**Compromised Account** https://support.google.com/accounts/answer/6294825 **Impersonation Account** https://support.google.com/mail/contact/abuse
Instagram	**Compromised Account** https://help.instagram.com/368191326593075 **Impersonation Account** https://help.instagram.com/446663175382270 **Live Streaming Issues** https://help.instagram.com/292478487812558
LinkedIn	**Compromised Account** https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account **Impersonation Account** https://safety.linkedin.com/identifying-abuse#profiles **Live Streaming Issues** https://www.linkedin.com/help/linkedin/answer/100225/broadcast-with-the-linkedin-live-feature

Service Provider	Contact Information
Microsoft Outlook / Microsoft Teams	**Compromised Account** https://support.microsoft.com/en-hk/help/10494/microsoft-account-how-to-access-a-compromised-account **Live Streaming Issues** https://support.microsoft.com/en-us/home/contact?ContactUsExperienceEntryPointAssetId=S.HP.teams
Snapchat	**Compromised Account** https://support.snapchat.com/en-US/a/hacked-howto **Impersonation Account** https://support.snapchat.com/en-US/i-need-help
Twitter	**Compromised Account** https://help.twitter.com/en/safety-and-security/twitter-account-compromised **Impersonation Account** https://help.twitter.com/forms/impersonation **Live Streaming Issues** https://help.twitter.com/en/using-twitter/twitter-live
YouTube	**Compromised Account** https://support.google.com/youtube/answer/76187 **Impersonation Account** https://support.google.com/youtube/answer/2801947 **Live Streaming Issues** https://support.google.com/youtube/answer/2474026
Zoom	**Live Streaming Issues** https://support.zoom.us/hc/en-us/articles/201362003 https://support.zoom.us/hc/en-us/articles/200613919-Reporting-abusive-behavior **Support Hotline** **Singapore**: +65 800 321 1249 (ext 2)

(back to top)

Cybersecurity Service Providers

Political parties should consider appointing a professional cybersecurity vendor to review and manage the cybersecurity posture for the party, as well as to deal with any cybersecurity incident. A non-exhaustive list of cybersecurity vendors who are CREST[1] members with a local office in Singapore and provides incident response services is provided for reference.

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

(back to top)

[1] CREST is an international not-for-profit accreditation and certification body that represents and supports the technical information security market