ADMM Cybersecurity and Information Centre of Excellence

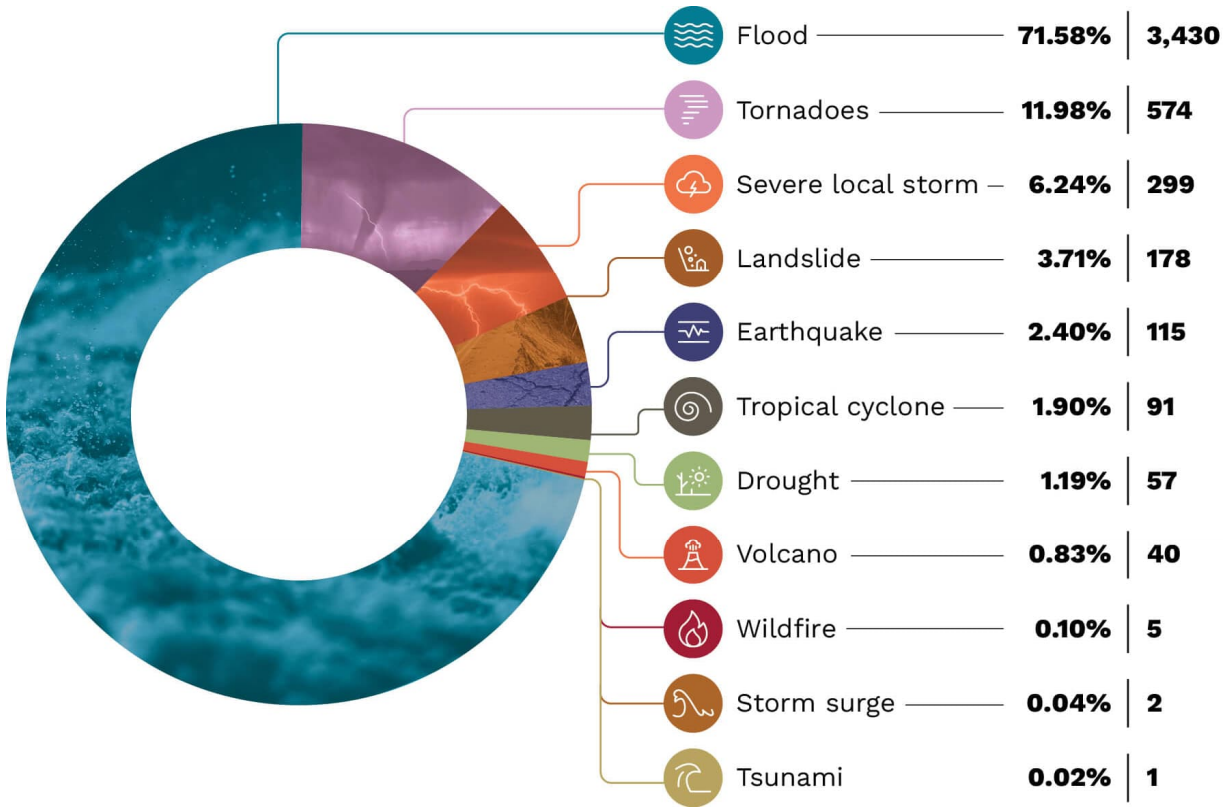
UPDATE ON
THE CYBER DOMAIN

Issue 4/24 (April)

Importance of Cybersecurity in Disaster Management

INTRODUCTION

1. Over 90% of natural disasters happening in the world are weather-water related including storms, drought, wildfires, pollution, and floods. Climate change is affecting the hydrological cycle, leading to increased frequency and severity of storms. Between 2012 and 2023, the ASEAN region was affected by over 4000 natural disasters and climate-related hazards – a number that is likely to increase given the continued upward trend of global temperatures.



Natural Disasters in ASEAN, 2012 – May 2023 (Source: ASEAN)

2. Reports by *Cloud Security Alliance* and *Insurance Business* highlight a spike in cyberattacks on individuals and organisations in the immediate aftermath of a natural disaster. The potential range of attacks varies widely – from cybercriminals impersonating disaster relief organisations to phish for personal information and financial gains; to malicious actors spreading misinformation and launching attacks on emergency services and critical infrastructures to cause chaos. This report will shine a spotlight on the reasons for the increase in cyberattacks during natural disasters, and highlight how organisations can adjust their cybersecurity posture in preparation for a range of crises, to enhance vigilance and be prepared for the cyber threats that may arise during and after the crisis.

INCREASE IN CYBERATTACKS DURING NATURAL DISASTERS

3. The uptick in cyberattacks and phishing attempts following a natural disaster can be linked to two reasons. **First**, the safeguards that protect IT infrastructure against cyberattacks may become non-operational when disasters destroy and disrupt critical information infrastructures (CII). This makes it easier for attackers to exploit vulnerabilities and launch cyberattacks. CIIs encompass vital systems and assets that are essential for the functioning of society, such as telecommunications, energy, defence, and transportation networks. During disasters like floods, storms and wildfires, key infrastructures like communication links may be severed, and power lines and data security operation centres destroyed. As a result, the safeguards which traditionally guard against cyberattacks become non-operational, offering opportunities for threat actors to exploit the chaos and launch cyberattacks against the operations of public and private organisations as they deal with the aftermath of the disaster.

4. **Second**, threat actors may take advantage of the chaos and information overload surrounding natural disasters to launch social engineering and phishing attacks against already-vulnerable individuals. In the modern age, many people rely on social media for their everyday news. However, their reliance on social media for information on the well-being of their family and friends significantly increased following the onset of disasters, as reported by the *Australian Institute for Disaster Resilience* in 2019. As people are exposed to more information than they can cope with, they may be less discerning about the information that they receive, thereby becoming more vulnerable to fraud, and more likely to fall for social engineering or phishing attacks. This can be exacerbated by the psychological and emotional stress that individuals are already experiencing.

5. Objectives of Cyberattacks During and After Disasters. Just like any other cyberattack, the motivations behind cyberattacks during and after natural disasters vary widely. However, common objectives include:

a. **Financial Gains**. Cyberattackers may take advantage of vulnerable people and individuals for a quick pay day through phishing, ransomware attacks, or data theft.

b. **Political Disruption**. Sophisticated threat actors may seek to use cyberattacks to disrupt government responses to the emergency, publicly embarrassing them with the aim of eroding political trust amongst its citizens.

c. **Cyberwarfare**. Malicious threat actors may take the opportunity to conduct large-scale cyberattacks to further harm another country in an already-weakened state.

PAST CYBERATTACKS CAPITALISING ON NATURAL DISASTERS

6. In 2014, cyberattackers hacked the US National Weather Service, forcing the US to cut the feed of satellite data, thereby disrupting global forecasting and monitoring models which were reliant on the data. In 2017, following the landfall of Hurricane Harvey on Texas and Louisiana, the US Computer Emergency Readiness Team (US-CERT) reported a 419% increase in phishing attacks, with millions of dollars lost to fraudulent charities and assistance programmes. Many of these attacks targeted individuals who had relatives in affected areas, and involved very personal content aimed at preying on one's emotions to increase the chances of success.

7. More recently, following earthquakes in Türkiye and Syria in 2023, cybercriminals posed as a charity foundation to fraudulently solicit for donations after the disaster, stealing personal information in the process. Moreover, hackers carried out distributed denial-of-service (DDOS) attacks against the communications networks used for NATO earthquake relief programmes for the Türkiye and Syria earthquakes resulting in a temporary disruption of search-and-rescue efforts.

Tue 2/7/2023 3:40 AM

Request for support for The Victims of Turkey Syria EarthQuake ...

To

Greetings s

We are launching support the people of Turkey and Syria who have been hit badly with The Ongoing Earthquake, this has displaced many families and children, leaving them homeless.

WLADIMIR FOUNDATION has taken it upon herself to render first hand Aid on ground to help as many people as possible..
We are urging you to please donate to Victims

for instant donation Please Use our automatic crypto wallets

ETH: (ERC 20): 0x7b7a546e432c7d8563
USDT (TRC 20) : TGKGgsRMgCoo5Pgn
BTC: 1L3bRtwJ3g3Vj8gJs8F

kindly visit our website to see some of our ongoing projects, and for other forms of donation please email support.

Thank You for your support

Wladimir Charity Foundation.

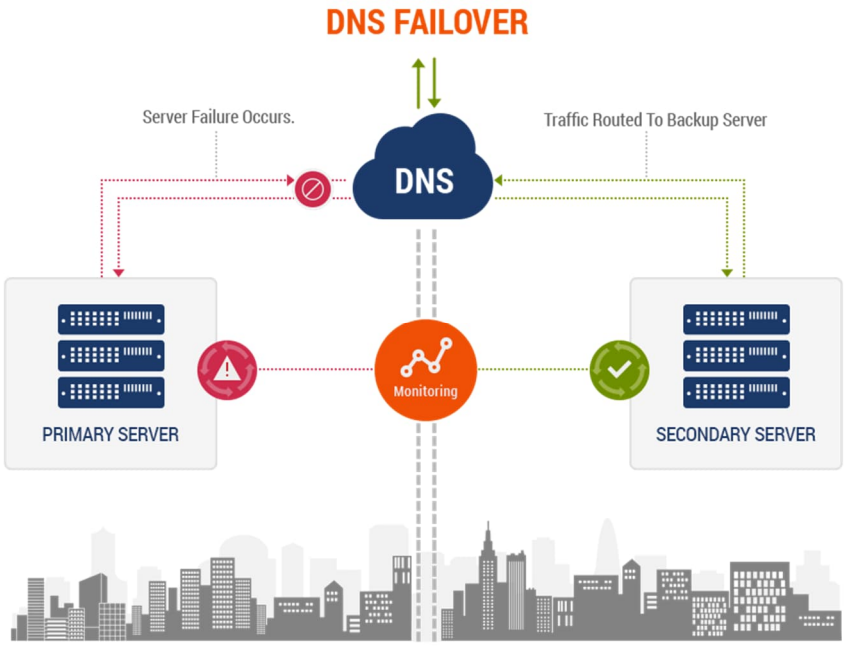
Phishing email by the fraudulent *Wladimir Foundation* (Source: Bitdefender)

RECOMMENDATIONS

8. It is therefore important for both public and private organisations to consider the impact of disasters – natural or otherwise – in their crisis cybersecurity plans. These plans should be comprehensive and sufficiently robust to cover a range of potential crises, from severe power outages to natural disasters and terrorist attacks. Having these plans in place would allow organisations to identify potential cybersecurity vulnerabilities and work towards mitigating their impact, thereby allowing the organisation to wholly focus on their response to the crisis at hand. Below are three recommendations which should be included in an organisation's cybersecurity plan:

Maintaining Geographic Redundancy

9. With organisations depending on the constant availability of their IT systems, redundancy data centres are increasingly being set-up to relieve the load on their primary systems and prevent failures. Geographic redundancy is achieved when data centres with replicated data are set-up with a large spatial distance between them. The location of redundancy data centres should not be in disaster prone areas, e.g., if an area is flood-prone, the data centres should not be located near the same river system, or within the same flood plain. Should the primary data centre fail due to a natural disaster, traffic can then be immediately routed to the backup server, preventing any disruptions to an organisation's operations.



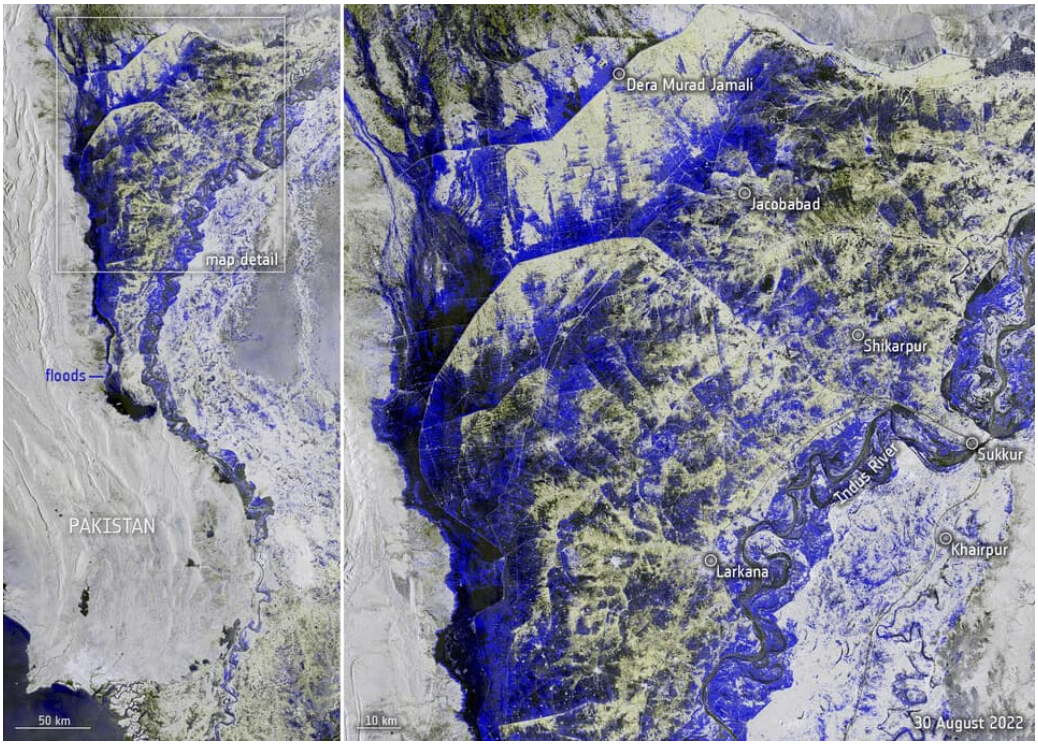
Geographic redundancy keeping systems online (Source: 2WTech)

10. However, the replication and storage of data across multiple sites also increases the number of potential vulnerabilities faced. Backup sites are often less-protected as compared to primary data centres, leaving them more vulnerable to cyberattacks. Additionally, as more personnel are needed to run the backup data centres, the chances of human error and social engineering attacks correspondingly increase. Organisations therefore need to ensure that redundancy data centres are outfitted with the same level of protection as their primary centres, while incorporating advanced data resiliency technologies to provide more protection and data recovery options across all their data centres.

Securing Communications and Monitoring Systems

11. As seen during the 2023 Türkiye and Syria earthquakes, cyberattackers may target and disrupt communication systems in the immediate aftermath of natural disasters to promote chaos. In disabling communications, they prevent first responders and government agencies from mobilising and coordinating recovery efforts after the disaster, taking advantage of the disruption to carry out large-scale cyberattacks or cybercrimes amidst the chaos. To guard against this, public and private organisations alike should ensure that their primary means of communications during a crisis are protected with end-to-end encryption, with backup systems readily available in the case of an attack.

12. Aside from targeting communication systems to promote chaos, cyber attackers may also target the monitoring systems used to provide early warning of natural disasters and support rescue efforts, as demonstrated in the 2014 cyberattack on the US National Weather Service. Organisations managing the disaster management services must ensure that the appropriate safeguards are included to protect the services from cyberattacks.



Flood maps captured by the EU's Copernicus Emergency Management Service, used to help first responders deal with the crisis (Source: European Space Agency)

Preparing Emergency Cybersecurity Plans

13. Noting the chaos that comes with any disaster, organisations need to think proactively and ensure that they have a comprehensive cybersecurity plan that is robust enough to withstand a crisis. To start, these plans need to clearly define the ways in which data is secured and protected from unauthorised access, and the roles of an organisation's employees in managing data access and cybersecurity in the immediate aftermath of a disaster. After the plans are created, organisations should rehearse the plans, to ensure that their employees remain familiar with the procedures, and that the plans are up-to-date.

14. These plans should also include measures to strengthen the fraud resilience of their employees during an emergency. Organisations should identify and assess likely fraud risks and data breaches that may emerge due to cybersecurity measures being removed for expediency (e.g., two-factor authentication) during the emergency. The associated consequences should be carefully assessed, with cost-effective controls introduced to compensate for the suspended measures. Finally, employees should be reminded to have their guard up when accessing suspicious emails and links, especially during times of emergency.

CONCLUSION

15. With instances of natural disasters likely to increase alongside climate change, public and private organisations alike need to ensure that their infrastructure and personnel are well-prepared for them. An organisation's crisis cybersecurity plan must be sufficiently robust and thorough to cover a wide range of crises, with emphasis placed on threats that an organisation may be more susceptible to (based on their location, status etc.), so that they are not caught unawares by opportunistic cyberattacks that exacerbate the crisis at hand.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

References

1. How to Maintain a Solid Cybersecurity Posture During a Natural Disaster [https://www.csoonline.com/article/1249508/how-to-maintain-a-solid-cybersecurity-posture-during-a-natural-disaster.html]

2. What's the Link Between Cyberattacks and Natural Catastrophes? [https://www.insurancebusinessmag.com/ca/news/cyber/whats-the-link-between-cyberattacks-and-natural-catastrophes-437350.aspx]

3. Natural Disasters: A Perfect Storm for Data Breaches [https://cloudsecurityalliance.org/blog/2023/12/11/natural-disasters-a-perfect-storm-for-data-breaches]

4. Cybercriminals Exploit Human Misery in Earthquake-hit Turkey and Syria with new Online Disaster Scam [https://www.bitdefender.com/blog/hotforsecurity/cybercriminals-exploit-human-misery-in-earthquake-hit-turkey-and-syria-with-new-online-disaster-scam/]

5. Watch out for Hurricane Harvey Phishing Scams [https://www.cbsnews.com/news/hurricane-harvey-phishing-scams-cybercriminals/]

6. Miscreants Sure Do Love Ransacking Cloud Networks More So Than Before [https://www.theregister.com/2023/01/20/cloud_networks_under_attack/]

7. The Role of Cybersecurity in Disaster Management [https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Space_for_Earth/The_role_of_cybersecurity_in_disaster_management]

8. Your Organisation is More Vulnerable to Fraud During a Crisis. Here's Why. [https://www.acfeinsights.com/acfe-insights/your-organization-is-more-vulnerable-to-fraud-during-a-crisis-heres-why]

9. Joining the Dots: Using Social Media to Connect with More Vulnerable Victorians During Emergencies [https://www.bnhcrc.com.au/sites/default/files/managed/downloads/peter_hayes.pdf]