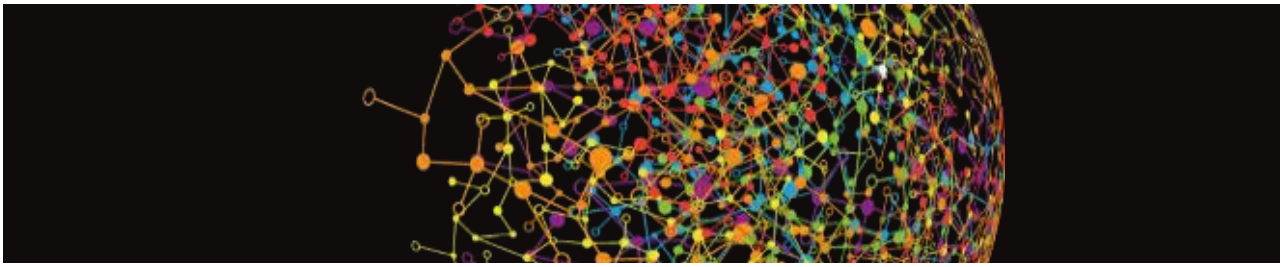
Deloitte.



COVID-19: Cyber considerations amid a global pandemic

What we are seeing...

As the effects of the Coronavirus are felt around the world, governments' and business's primary focus is the safety of their citizens, employees and customers. Meanwhile, cyber attackers are impersonating health organizations (for example. World Health Organization[1], healthcare organizations etc) and other government entities, in malicious email campaigns designed to invoke fear, hoping to trigger action that will provide them opportunity to gain access to systems and sensitive information. A carefully considered approach will enable an organization to proactively address cyber challenges during an extraordinary event. The below offers a few cyber considerations for organizations to think about as they align their strategies and workforce around COVID-19.

Cyber Considerations amid extraordinary events

As organizations recommend employees work remotely there is increased use of mobile devices and remote access to core business systems | Strengthen organizational Identity Access Management and SEIM monitoring

Cybersecurity risks increase with more encouraged work from home. Proactive measures may enhance user experiences and security for remote access, safety enabling opportunities for telework. Unprotected devices could lead to the loss of data, privacy breaches, and systems being held at ransom. Organizations should:

- enforce a consistent layer of multi-factor authentication (MFA) or deploy a step-up authentication depending on the severity of access requests.
- ensure identity and access management processes fully secure third-party identities access networks.
- have a comprehensive view of privileged identities within their IT environments, including a procedure to detect, prevent, or remove orphaned accounts.

Crises often lead cyber adversaries to take advantage through malicious schemes | Increase awareness of threats

Phishing campaigns related to COVID-19 are increasing and well disguised as reputable health organizations, for example. Organizations should remain vigilant for scams related to Coronavirus Disease 2019 (COVID-19). Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Attacks like these can propagate quickly and extensively impact an entire enterprise network, cause identity theft and submissions of fraudulent claims for payments and benefit programs.

Tips to avoid a "phishing" expedition

- Exercise caution in handling any email with a COVID-19 related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.
- Use trusted sources—such as legitimate, government websites for up-to-date, fact-based information about COVID-19.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

Coronavirus malware campaigns since January 2020

- Coronavirus themed Malspam with attached ISO disk image file delivers LokiBot
- Coronavirus themed Malspam delivers Remcos RAT
- Attack campaign leverage Coronavirus (COVID-19) theme to deliver Remcos RAT
- Coronavirus themed malspam delivers Formbook
- New Patchwork malspam campaign with maldocs themed for coronavirus and Chinese individuals
- Coronavirus themed Malspam delivers Emotet"

Digital transformation enables organizations to evolve security safeguards and systems to prevent intrusion and access to critical systems | Cyber Recovery

In an era of cyber everywhere, with more technological transformation, use of cloud, and broader networking capabilities, the threat landscape continues to increase and cyber-criminals will look to attack operational systems and backup capabilities simultaneously in highly sophisticated ways leading to enterprise-wide destructive cyberattacks. Organizations can improve their defense posture and attack readiness with good cyber hygiene, incident response strategy, architecture and implementation of cyber recovery solutions to mitigate the impact of cyber-attacks. A viable cyber resiliency program expands the boundaries of traditional risk domains to include new capabilities like employee support services; out-of-band communication and collaboration tools; and a cyber recovery vault.

No matter the event or circumstance, Deloitte helps organizations to strategically prepare for, respond to, recover and transform from high-consequence cyber incidents that could seriously disrupt operations, damage reputation, and destroy shareholder value. Cyber strategies should converge across business, operations, business continuity/technical resilience, and crisis management functions as well as employ unique methods that reveal network exposures, detection of advanced threats, and discovering systemic Incident Response process gaps.

Contacts

Rohit Mahajan
President – Risk Advisory
rmahajan@deloitte.com

Gautam Kapoor
Partner
gkapoor@deloitte.com

Ashish Sharma
Partner
sashish@deloitte.com

Gaurav Shukla
Partner and Leader
Cyber, Risk Advisory
shuklagaurav@deloitte.com

Vishal Jain
Partner
jainvishal@deloitte.com

[1]World Health Organization (2020) https://www.who.int/about/communications/cyber-security