CHECKLIST

PANDEMIC
CYBER LOSS PREVENTION – INFORMATION SECURITY

This document is intended to provide cyber loss prevention guidance for organizations operating during a pandemic event. Keeping your company running may require approaches outside of "business as usual", with heavy reliance on remote work and adjusted schedules and engagement practices. Along with the circumstances surrounding a pandemic event, these deviations present unique cybersecurity challenges. However, with appropriate cyber vigilance and awareness you can effectively reduce the likelihood of a successful cyberattack on your organization.

Cyber criminals continue to leverage social engineering and phishing tactics to gain unauthorized access to company networks. In fact, phishing remains the most prevalent attack delivery method and infection vector for malware and ransomware.

Use these guidelines to help focus your cyber loss prevention efforts during the pandemic, in line with established company policies.

SOCIAL ENGINEERING

As a pandemic disrupts enterprises and impacts cyber security, threat actors are exploiting businesses with social engineering attacks. Safeguard yourself and be watchful for an email, phone call or online message with compelling stories such as:

- ☐ A problem that requires your "verification" using your personal information
- ☐ Urgently asking for your help
- ☐ Notification that you won something significant, such as a lottery or raffle
- ☐ Email originating from your manager or co-worker, asking for internal, sensitive information

PHISHING

In an attempt to gain unauthorized access to your company networks, cyber criminals may lure you to a seemingly legitimate website that they control, make job offerings that promise easy extra money, or ask for charity donations to fake organizations affected by a pandemic. Some steps to mitigate the threat of phishing include:

- ☐ Be as watchful and mindful as you are in the office when opening foreign emails or attachments at home
- ☐ Utilize only familiar websites where there is less likelihood of hosted malicious content
- ☐ Check the source of emails
- ☐ If in doubt, don't risk it. Call your Information Security and/or IT support

The anxiety related to this unprecedented situation may lead users to click on pandemic-related phishing emails that could release malware into the organization.

FM Global

PANDEMIC PROPERTY LOSS PREVENTION CHECKLIST

VIDEO CONFERENCING

Cyber criminals can discreetly hack and steal confidential information being shared on business meetings held via video conferencing software, jeopardizing company information in a way that could impact operations. Where possible, consider these safeguards:

- ☐ Disable the default setting that allows meeting participants to share their screen without permission from an event's host
- ☐ Enable password protection to prevent uninvited users from joining
- ☐ Require host to be present before meeting starts
- ☐ Close unrelated applications and documents before sharing your screen, to prevent unintended disclosure
- ☐ Only allow individuals with a given e-mail domain to join

PATCHING

Cyber criminals will attempt to exploit known vulnerabilities within operating systems and applications. With an increasing trend of employees using their own devices for business purposes and remote work, it is especially important to be cautious with the data accessed or stored on these devices. To safeguard devices and help protect data:

- ☐ Keep operating system(s) versions and patches up to date
- ☐ Where possible enable or require automatic updating
- ☐ Validate anti-virus and anti-malware software are patched and updated with the latest versions
- ☐ Consolidate software versions whenever possible between home and office
- ☐ Secure any device that might be able to integrate with corporate networks and services

USEFUL RESOURCES

Home working: preparing your organisation and staff
https://www.ncsc.gov.uk/guidance/home-working

Home and Business resources
https://www.us-cert.gov/ncas/tips/ST15-002

Understanding Patches and Software Updates
https://www.us-cert.gov/ncas/tips/ST04-006

Keep your computer safe at home
https://support.microsoft.com/en-us/help/4092059/windows-keep-your-computer-secure-at-work

EXTERNAL LINKS DISCLAIMER

Although every effort is made to ensure these links are accurate, up to date and relevant, FM Global cannot take responsibility for pages maintained by external providers.

FM Global

For additional copies of this publication or other FM Global resources, order online 24 hours a day, seven days a week at fmglobalcatalog.com. Or, for personal assistance worldwide, contact our U.S.-based customer services team:

- Toll-free: (1)877 364 6726 (Canada and the United States)
- Phone: +1 (1)401 477 7744
- Fax: (1)401 477 7010
- E-mail: customerservices@fmglobal.com