Cyber

Ransomware Supplement

Instructions: For any questions answered "No," please consider providing additional information in the comments section on the last page.

1. Do you take the following steps to protect your network from ransomware:

- Apply security patches within 30 days of release? ○ Yes ○ No
- Tag external emails to alert employees that the message originated from outside the organization? ○ Yes ○ No
- Implement SPF, DKIM and DMARC to protect against phishing messages? ○ Yes ○ No
- Utilize Web filtering to block access to known malicious websites? ○ Yes ○ No
- Segment your network based on the classification level of information stored on said systems? ○ Yes ○ No
- Utilize any unsupported operating systems or platforms? ○ Yes ○ No
- Utilize an advanced endpoint detection and response (EDR) tool? ○ Yes ○ No
- Utilize a SIEM monitored 24/7 by a SOC? ○ Yes ○ No
- Have a process to decommission unused systems? ○ Yes ○ No
- If Office 365 is used, do you utilize the O365 Advanced Threat Protection add-on? ○ Yes ○ No
- Implement PowerShell best practices as outlined in the Environment Recommendations by Microsoft? ○ Yes ○ No

Additional comments:

2. Do you take the following steps to protect your employees from ransomware:

- Conduct security awareness training at least twice a year? ○ Yes ○ No
  - How frequently? _____
- Conduct phishing campaigns at least quarterly? ○ Yes ○ No
  - How frequently? _____
- Ensure employees utilize least privilege at all times, and **do not operate as local administrator?** ○ Yes ○ No
- Do you require multi-factor authentication: ○ Yes ○ No
  - For remote access to the network? ○ Yes ○ No
  - To protect privileged user accounts? ○ Yes ○ No
  - For all cloud resources, including Office 365? ○ Yes ○ No
  - For all Remote Desktop Protocol (RDP) and virtual desktop instances (VDI)? ○ Yes ○ No

Additional comments:

3. Do you take the following steps to protect your data from ransomware:

a. Regularly perform full and incremental backups of business data?	Yes	No
b. Test backups for restorability?	Yes	No
c. Ensure backups are stored physically offsite?	Yes	No
d. Ensure backups are stored offline to safeguard from infection?	Yes	No
e. Have an annually tested incident response plan with the ability to quickly contain an incident?	Yes	No
f. Have formal disaster recovery and business continuity plans that are annually tested?	Yes	No

4. Do you take the following steps to protect your organization from a vendor compromised with ransomware:

a. Have a formal vendor management program that inventories and classifies the type of data and level of access each vendor has?	Yes	No

Where necessary based on the risk classification:

b. Contractually require third parties to protect this information with safeguards at least as good as your own?	Yes	No
c. Perform due diligence on each such 3rd party to ensure that their safeguards for protecting sensitive information meet your standards (e.g., conducting security/privacy audits or reviewing findings of independent security/privacy auditors)?	Yes	No
d. Audit all such third parties as necessary to ensure that they continuously satisfy your standards for safeguarding sensitive information?	Yes	No
e. Contractually require them to defend and indemnify you if they contribute to a confidentiality or privacy breach?	Yes	No
f. Require them to either have sufficient liquid assets or maintain enough E&O insurance to cover their liability arising from a breach of privacy or confidentiality?	Yes	No

Additional comments:

_____

_____

_____

Please describe any additional controls, training or steps that your organization takes to identify and mitigate ransomware attacks:

Signature:_____

Print name: _____

Title: _____

Company: _____

Date (mm/dd/yyyy):_____

For more information, please contact your local CNA underwriter or visit our website at cnacanada.ca.