CYBER INCIDENT PREPAREDNESS CHECKLIST

I. *Before* a cyber intrusion or attack

A. Identify mission critical data and assets (your "crown jewels") and institute tiered security measures to appropriately protect those assets.

B. Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework

C. Have an actionable plan in place before an intrusion occurs

Test Plan with (scheduled) exercises

Keep plan up-to-date to reflect changes in personnel and structure

D. Have appropriate technology and services in place before an intrusion occurs

E. Have appropriate authorization in place to permit network monitoring

F. Ensure your legal counsel is familiar with technology and cyber incident management to reduce response time during an incident

G. Ensure organization policies align with Incident Response (IR) plan

H. Engage with law enforcement before an incident

I. Establish relationships with cyber information-sharing organizations

II. *After* a cyber intrusion or attack

Step 1: Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch

Step 2: Implement measures to minimize continuing damage

Step 3: Record and collect information

Image affected computer(s)

Keep logs, notes, records, data

Record any continuing activity/attacks

Step 4: Make appropriate notifications to

Personnel within a company or the organization

Federal and State law enforcement

Regulators – Local and Homeland Security

Other Potential victims

Step 5: Review response and remain vigilant

- Continue monitoring the network for any anomalous activity to make sure the Intruder has been expelled and you have regained control of your network

- Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan

CYBER INCIDENT PREPAREDNESS CHECKLIST (cont'd)

III. What not to do following a cyber intrusion or attack

A. Do not use the compromised system to communicate
B. Do not try to 'fix' this yourself
C. Do not hack into or damage another network
D. Think that the problem is solved after you correct
E. Start using the repaired system or computer
F. Think that this will never happen again
G. Believe that your other systems and computers are 'safe'

AGENCY RECAP

If something looks strange or if you know a breach has occurred

☐ Do not try to "fix" this yourself
Contact your manager
Send a notice to all your co-workers

☐ Contact your Bank(s) right away
Make them aware - Have them place a 'freeze' on the account

☐ Contact your Underwriter(s)
We can get you into contact with our National Settlement Services Team
We can get you into contact with our Fraud Resolution and Legal Teams

☐ Contact everyone in the Transaction (must give 'Notice')
Find where the breach occurred
You may be able to find out additional information that could be helpful

REMEMBER THAT FRAUD, CYBERCRIME OR A BREACH CAN BE OF FILE DATA, CONTRACTS, LOAN DOCUMENTS, ANY FORM OF MONEY, ANY NPI, ANY NPPI

Brought to you by: Linda Grahovec NTP, VP Director of Education and Marketing for FNTG Underwriters
Reference: USDOJ.gov – Cybersecurity Unit – Best Practices for Victim Response and Reporting of Cyber Incidents