WHEN THE CYBER ATTACK HAPPENS

WHAT TO DO in the first 24 hours……

CHECKLIST

☐ **First Call -** Mobilize your Incident Response/Cybersecurity Response Team

☐ **Contact and Retain Cyber/Privacy Counsel** – Ensure Confidentiality of the Initial Investigation

☐ **Contain the Pain** – Take action to stop or contain the attack

- Block further intrusion into the network/data stores
- Disable remote access to the network/Re-route network traffic
- Preserve all Indicators of Compromise/System Logs

☐ **Alert and Engage -** Trusted, tactical third-parties

- Managed Service Partners (IT)(SOC)
- Forensic Investigation Provider
- Crisis Management/Communication Team

☐ **Identify the Attack** – Identify the type of Incident or Cyber-attack

☐ **Notify your Cyber-Insurance Carrier**

- Advise the carrier, in writing and verbally, of the incident
- Validate what expenses and losses the policy covers
- Determine what actions the policy requires of the business

☐ **Notify the Appropriate Legal/Regulatory Authorities**

- FBI
- Secret Service
- DHS
- Local law enforcement

☐ **Notify Impacted Customers/Partners** – Based on External Impact

- Provide enough detail so they can protect against any downstream threat
- Advise customers/partners of impact on your service delivery and timeline of return to service
- Prepare to provide all regulatory/legal notifications required by law or by contract

Heidi J.K. Fessler
Innova Law Group, PLLC
hfessler@innovalawgroup.com
651.278.3895

John Cannady
NUARI
jcannady@norwich.edu
404.499.6849

Seamus Leary
Meridian Strategic Services, Inc.
sleary@meridianstrategicserv.com
845.332.5599