Cybercrime Pre-Breach & Post Breach Checklist

SNELLINGS WALTERS INSURANCE AGENCY

MIS

PRE-BREACH

Cybersecurity Services and Audit	Hire an expert and have the proper security controls and processes in place to protect your company. Your insurance carrier or broker can suggest many available companies to work with. Establish a relationship and have their contact information available (hard copy) other than on your computer / network. • Employee Cybersecurity eLearning and Phishing Simulation • Blacklist IP Blocking and Domain Protection • Infrastructure Vulnerability Scan • Endpoint Detection and Response • Processes for Containment • Forensic Risk Consultation • Rigorous external 3rd party security testing and risk assessment (at least annually, quarterly preferred)
Legal Risk Consultation	Many insurance carriers will provide a list of local firms familiar with cyber claims. Contact an expert and have a conversation / meeting to establish them as your post-breach resource. Have their contact information available (hard copy) other than on your computer / network. • Incident Response Planning • Regulatory Compliance • Public Relations Risk Consultation • Crisis Communication Plan • Educating Staff on Time-sensitive Crisis Management
Insurance Portfolio Assessment	Have a knowledgeable broker review your policies for necessary endorsements, or add new coverages. Have their contact information available (hard copy) other than on your computer / network. • Top rated insurance carriers will have a cyber response team available for you, including a Cyber Coach • Review of your property and casualty portfolio to determine how it's anticipated to respond to the spectrum of cyber-predicated financial and tangible losses • Cross reference policy gaps and overlaps as related to cyber with errors and omissions, Ccime policies etc. • Have adequate coverage for 1st party damages and 3rd party damages. • Insure with the right limits. Small companies can be devastated by million-dollar claims • Review contracts and insurance coverages with IT infrastructure & software vendor • All clients, suppliers and vendors should have comparable and adequate insurance as well

Ralph Pasquariello, CLCS
Snellings Walters Insurance Agency
770-396-9600
rpasquariello@snellingswalters.com

POST-BREACH

Contacting your pre-breach contacts will jump start you on defending the attack both physically and financially. If preparations were not made or cannot be reached, the law enforcement contacts below are specialists in cybercrime. Local police departments are also ramping up their teams to include a cybercrime division.

Law Enforcement	**FBI** https://www.ic3.gov	**U. S. Secret Service** Electronic Crimes Task Force DC (202) 406-5708 Electronic Crimes Task Force Atlanta (404) 331-6111 https://www.secretservice.gov/investigation	**GBI** GA Cyber Crime Center - Augusta Special Agent Steven Foster Steve.Foster@gbi.ga.gov (706) 941-5400

Cybercrime Has Many Faces

The wide variety of malware (millions of versions) and elusiveness of cyber criminals makes it almost impossible to avoid an incident. There are dozens of attack points and endless versions of malware:

- Ransom Attacks
- Data Exfiltration
- Crypto Mining
- Fraudulent Instructions, Currency Transfers
- Invoice Manipulation
- Business Email Compromise
- Data Destruction and Business Interruption

Response to an Attack

Due to variations and vastness of attacks, there is no single answer to the response or reaction to a cyberattack. Malware and criminals can wander through your computers network for many months undetected. The average discovery time is actually over 200 days. With the help of the industry experts the methods they will use follow a protocol to do the following:

- Containment
- Eradication
- Restoration

Recovery After a Cyber Event

Many small companies never recover after a cyberattack.

With a process in place, you will be more equipped to handle the event when it happens. Many companies go through cyber drills to prepare (much like a fire drill).

Business interruption can sometimes take months or years to recuperate. (Physical damage to computers "bricking", data loss.)
Reputational harm can also cause financial distress.

Reaction time is critical. Use your resources to recover.