CYBER INSURANCE MADE EASY™

COWBELL™
CYBER

You Discover a Cyber Incident - What Now?

1. **Develop a summary or timeline of events** leading to the discovery of the cyber event.
2. **Track all costs,** if any, that you have incurred to date associated with the cyber event.
3. **Estimate the number of devices** and/or endpoints on your network.
4. **Report to Cowbell: (833) 633 – 8666 (ext. 702)**
   Ransomware hotline: (844) 578-0219

- The above will give you access to experienced incident response teams - including breach counsel, ransom negotiators, and data recovery specialists. This will accelerate the return to normal operations.

- Provide Cowbell contact information for necessary decision makers and interested parties - business owners, executive officers, internal IT professionals, security officers, and/or any third party IT or security providers.

- Specifically, you should provide:
  - The date and time the potential cyber event was discovered,
  - A basic summary/timeline of the facts associated with the event,
  - Any remediation efforts undertaken,
  - Any vendors and/or attorneys retained, and
  - Any financial loss experienced to date.

You Discover a Cyber Incident - What Now?

If you have experienced a wire fraud event:

- Collect all communications that you suspect may have led to the event.
- Gather banking information or transaction confirmations documenting the transfer.
- Provide contracts related to the potential wire fraud event.

If you have experienced a email breach event:

- Develop an outline of customers' information and data that might have been sent, stored, attached, etc. to your email system, including invoices, contracts, and/or personal information of employees, customers, or partners.

If you have experienced a ransomware event:

- **Do not engage the bad actor.** Cowbell's team will assist with any ransom negotiations.
- **Do not attempt to restore from backups.** Cowbell will provide experts to ensure that your system is safe and secure prior to any restoration.
- Determine if you have any legacy and/or specialty equipment or software that may have been affected by the event.
- Develop an outline of sensitive data or information that your system may contain that may have been affected by the event.

STAY IN CLOSE CONTACT WITH COWBELL AND THE CLAIMS-HANDLING TEAM THROUGHOUT THE PROCESS (IMMEDIATELY RESPOND TO EMAILS AND CALL THEM BACK!)

Cyber Insurance Made Easy

Cowbell Cyber delivers standalone, individualized and state-admitted cyber insurance to small and mid-size businesses. Cowbell's cyber policies include risk management resources, including risk insights and assessment, breach coaches, and cybersecurity awareness training.