Cyber Incidents and Resulting Damages

Cyber incidents and damages caused by cybercriminals can take many shapes. We have listed below terms and wording that you should get familiar with when evaluating a cyber insurance policy. A data breach is only one of the many types of damages inflicted by a cyber incident.

Types of Cyberattacks, Cyber Incidents or Damages	Description
Social Engineering Attacks (BEC, Phishing, Banking Fraud, Wire Transfer fraud)	Social engineering is defined as a malicious action that causes a deviation from standard operating procedures or policies and subsequent losses by the organization. Examples include emails, phone calls from a fake help desk, and the presentation of counterfeit credentials or badges to gain physical entry to a restricted space.
BEC (Business Email Compromise)	BEC is defined as a criminal impersonating an employee by sending emails that pretend to be sent from the employee. This is a highly personal attack. The danger of this type of attack is that it exploits gaps in the insured's processes resulting in banking fraud, wire transfer, ACH, or theft of money.
Phishing Attacks, Whaling (targeted at people with privileged access), Smishing (SMS), Vishing (Voice)	Phishing is defined as an email scam meant to trick the recipient into clicking on a malicious link or downloading a piece of malware that enables the criminal to access personal or company information. This is a non-personal attack. Sending thousands of emails in hopes of tricking a few.
Banking fraud	Banking fraud stems from a social engineering attack where banking information is compromised and stolen from a person or business to steal money.
Ransomware	Cyber criminals infiltrate the company's digital infrastructure and freeze all activity on some computers or systems until a payment is made (usually with cryptocurrency).
Hacking/ Malware (ex.: Virus)	Hacking is when an outsider breaches a computer system or database and installs malware that disrupts or destroys a computer system.
Rogue employee / Malicious insider	This is when an employee or company insider uses the access rights they have to company assets to launch a cyber attack on the company.
Lost / Stolen Device	A company device (phone, tablet, computer, server, backup tapes) is lost or stolen.
W-2 Fraud	This occurs when a data breach compromises W-2 forms which have Social Security Numbers on them. SSN is a type of data subject to numerous privacy and security regulations. SSN compromise can lead to regulation fines.

Legal and 3rd party actions	These are the costs associated with forensic analysis to determine security breaches, or for legal action because of a security breach.
Distributed Denial of Service (DDOS)	A distributed denial-of-service attack is a cyberattack in which the perpetrator seeks to make an internet-connected machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting the service by overwhelming the resource with unintended requests.
Office Productivity software exploits	This is where hackers exploit cloud-based business applications to steal company information
Losses Due to Non-Criminal Factors	The following losses are due to internal errors that are made within the company that are done without criminal intent.
Staff Mistakes	These are mistakes made by staff that result in systems breaking or going down. This is not done with intent/criminal behavior.
System Misconfiguration	It is not uncommon for systems or cloud infrastructure to be deployed with security misconfiguration (human error or oversight) allowing cybercriminals to intrude on the system. Example: S3 buckets storing data left opened to public access.
Network Intrusion using an Exploit of a Known or Unknown (zero-day) System Vulnerability	Software and systems can have “bugs” (memory leaks,...) that cybercriminals can use to intrude into an organization's network and systems and deploy a cyber attack. Such errors are especially troublesome insofar as they often remain latent in effect, and the incidents arising from them might occur months or even years after the initial error. Recent example: Microsoft Exchange hack
System Glitch/Hardware Malfunction	This is caused by a malfunction in hardware that takes down a company's systems. This is a rare claim that is most commonly just categorized as a programming error
Mishandling of paper records	The mishandling of paper records that could potentially get into the hands of the wrong people, where cybercrime can stem from.
Wrongful Data Collection	Wrongful data collection is the collection of data without consent in the case the data is subject to security and privacy regulations that require such consent prior to collection.
Trademark/ copyright infringement	Trademark infringement is the unauthorized use of a trademark or a service mark in a manner that causes confusion, deception, or mistake about the source of the goods or services. Copyright Infringement is the use of copyrighted content without having the explicit consent of the owner to use the content.

Disclaimer: The examples and descriptions provided above are for general, informational purposes only. Notably, these descriptions do not set forth all possible scenarios and/or situations applicable to the described events. Policyholders should always refer to their own Policy for specific terms and definitions applicable to their Policy. Nothing in this document is intended to describe or define any coverage offered by Cowbell. However, should you need further information or assistance, please do not hesitate to reach out to us at Cowbell - we would be happy to help with any questions or concerns that you may have.