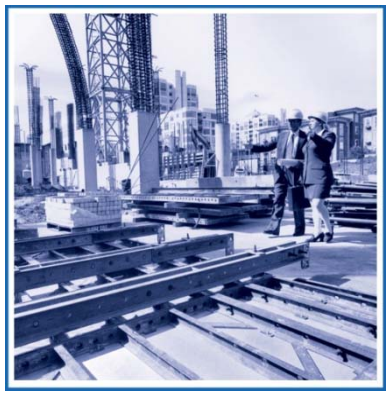
CONNER STRONG & BUCKELEW



“Cyber” Insurance

WHAT it is, and **HOW** it works…..

2018 NJ-GMIS TEC

What is

really?

Cyber Insurance Overview

1st Party

- Ransom
- Restoration
- Interruption
- Legal, Forensics
- Third Party Management

3rd Party

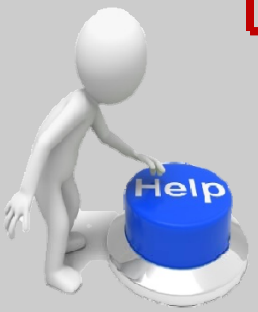
- Privacy Liability
- Security Liability
- Regulatory
- Media Liability
- Professional Liability

Incident Response

- Professionals: Coach, Legal, Forensics
- Notifications to Affected Individuals
- Credit Monitoring
- Public Relations

Cyber Incident Roadmap

You expect or know of a cyber incident. The clock is ticking to avoid further damage to you and your stakeholders.



Step 1 Report to Claims Manager

Step 2 Call Your Insurer's breach hotline @ 1-800-INSURER

Cyber Claims Coach steps in to manage the claim for you

When needed, your Cyber Claims Coach will engage an Insurer preapproved expert cyber attorney

In addition to their duties, the attorney will engage any other needed experts (i.e. forensics)

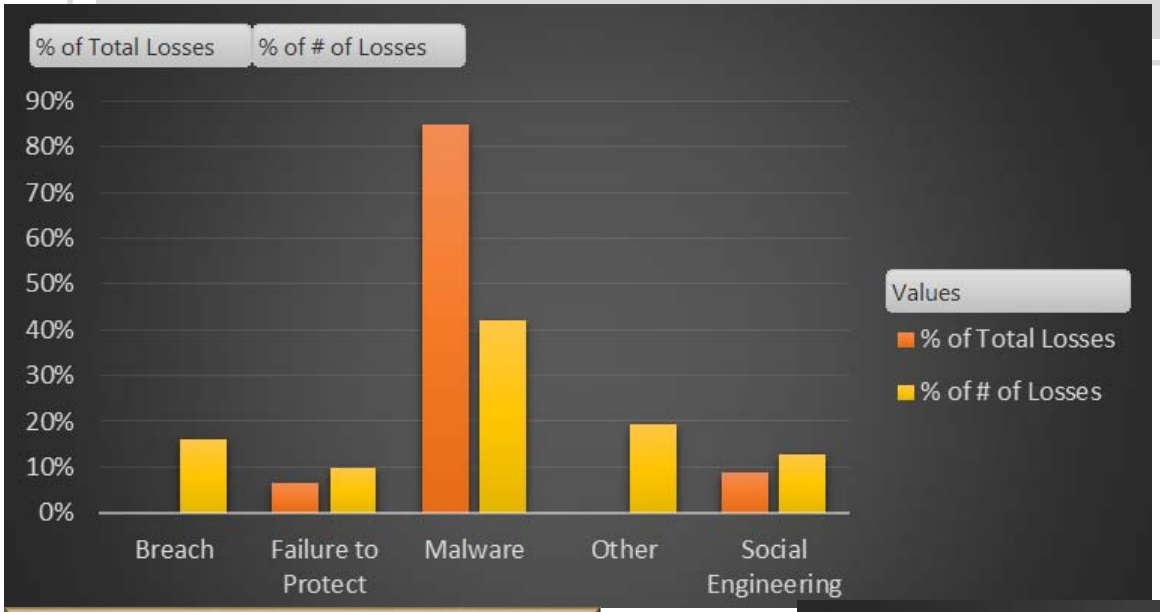
Your Cyber Claims Team will walk you through every step of responding to the incident and offer assistance and take actions on your behalf as necessary.

CITYTOWN

Other Considerations

Your Cyber Insurer
www.YourCyberInsurer.com

2017 Public Entity Cyber Trends



By Event Type

$71 per capita cost of a data breach for the Government Sector (2nd)
2017 Ponemon Institute

By Department

53% of data breaches were caused by human error or system glitch *2017 Ponemon Institute*

CONNER STRONG & BUCKELEW

2017 Public Entity Cyber Trends

Claims Examples

Social Engineering

A treasurer received an email looking to be from a senior employee requesting a wire transfer be made to an address included in the email for a particular project for the entity. Deception: 1) Looked like it was from the senior employee as the email address was spoofed; and 2) Seemed to be for a sound purpose. $20,000 was sent to the fraudster.

Ransomware

An administrative employee of an entity clicked on a "spoofed" link in a fake email, downloading the ransomware to the infected device and other devices it could spread to on the network. The entity had daily backups, but the backups were performed on the same network. As such, the lost data could not be reconstructed. Breach counsel and forensics were engaged. Total loss neared $70,000.

Malware

Malware downloaded via a spoofed email onto an employee's workstation. Since the workstation was open to a shared server, including a shared drive, multiple workstations were affected. Breach counsel and forensics were engaged, determining the personal information of nearly 1,000 individuals was compromised, triggering state notification regulations. The individuals were notified, and a call center and a credit monitoring account were setup for the affected individuals. Total loss in excess of $120,000.

Breach / Ransomware

A network connected printer ("IoT" device) had an "open port" to the internet. An intruder gained access to the entity's network via the open port and downloaded Ransomware onto the network. Breach counsel and forensics were engaged. Total loss in excess of $50,000.