Cyber Claims
Notification Process

Your company discovers a Cyber Security breach, **now what?**

You suspect that you have been the victim of ransomware, unauthorized access to, or the misuse of, modification to the network, and/or denial of network resources by attacks perpetuated through malware, spyware, or the like.

What should you do next?

1 Your company has suffered a security incident. The clock is now ticking. It is time to do right by your customers, employees, shareholders and all stakeholders. A quick response will save from lawsuits and regulatory inquiries

2 Immediately gather your internal team and review your incident response plan.

Current Claims Contact:

Richard Kissel
Kissel Hirsh & Wilmer LLP
rkissel@kphwlaw.com
Phone: (914) 750-5933

OR

Clark Hill Cyber Response 24 Hour Hotline 877-912-9470

3 Debrief with the claims team assigned to you. Important items to communicate:

1. What type of event occurred?
2. Was there a lost device?
3. Was this a malicious attacker?
4. Was this a disgruntled employee?
5. What if anything has the company done since the event happened?

4 The Claims specialist will help you formulate your response:

1. Engagement of pre-approved expert privacy attorneys to determine legal applicability of actions to respond to reporting requirements and maintaining privilege
2. Engagement of computer forensics to determine existence, cause and scope of breach
3. Do we need to hire a public relationships or crisis communications form?