

Cyber Risk Checklist

Example/Notes

Importance 1-10

A virus infects your network. It sends out email messages to your contacts. Several of your contacts become infected by the same virus when they open these emails.	
A disgruntled employee/volunteer who has inside access to your computer systems decides to destroy your data and attack your network.	
You sign a non-disclosure agreement regarding confidential information. A data breach causes this information to be released. You are now in violation of the contract.	
You store your information in the cloud. Your cloud provider is breached causing your confidential data to be disclosed.	
Your employee posts a defamatory message on a social media website unrelated to your company's website or marketing material. Legal action is brought against your organization.	
Legal action is brought against your organization for trademark infringement because your logo and visual style are considered infringing by a third party.	
Your office is broken into. Computers are physically taken but also paper files containing confidential information. This information is now breached.	
An unencrypted laptop containing sensitive information is stolen from your executives car while parked. It was not connected to your network at the time.	
You have clients in other States. Due to a data breach that contains PII you now must comply with regulations and laws of these states. This includes required notification of affected individuals.	
Malware shuts down your organization's computer operations. There is no physical damage to your computer network but the disruption in your operations will impact your financials.	
A breach affects your clients and stakeholders. You pay to notify the affected individuals and offer credit card monitoring even if you are not legally required to do so.	
A breach of confidential information has negatively effected the reputation of your organization. You hire a public relations firm to minimize the damage.	
Your instructed by your vendor to send remaining payments to a new account. Your accounting department sends payment only to find out that the vendors email was hacked and the funds have been sent to a cyber criminal.	

Howard Miller, CRM, CIC
 VP, Director of Tech Secure® Division
 L/B/W Insurance & Financial Services, Inc.
 (661) 702-6039
howardm@lbwinsurance.com
www.lbwinsurance.com

L/B/W is an independently owned agency providing complete commercial insurance and group benefit programs since 1922. We serve a broad range of companies in professional services, general business, nonprofit and the technology sector.

* Not a complete list. Always consult with the appropriate professionals for your organization's