# Technology Claim Scenarios

CNA NetProtect Essential℠ provides Privacy, Identity Theft and Network Security Liability coverage for any company that relies on electronically stored information. Simple, daily tasks, such as storing sensitive information on your network or connecting to the Internet, make your network a resource that can be exploited by criminals. Below are claim scenarios that depict how CNA NetProtect Essential℠ may help protect your technology business.

A mid-sized technology company hosts Web sites for retailers. Retailers rely on Web site availability to generate e-commerce income. The technology company's site is disrupted by a virus. Its customers' ability to generate income is disrupted. Customers sue the company to recover lost income.

A circuit card contract manufacturer relies on its network to operate its production line. The network becomes infected by a computer virus, which disrupts production and causes a delay in delivery of a customer's order. The customer sues the manufacturer for consequential damages, seeking recovery of late delivery penalties imposed by the customer's clients.

A circuit card contract manufacturer stores its customer's design information on its network to support production of custom assemblies in accordance with customer specifications. A computer virus corrupts the customer's specifications. As a result, the contract manufacturer produces parts that deviate from customer specifications. This delays the customer's deliveries. The customer sues the manufacturer seeking recovery of late delivery penalties imposed by its downstream customer.

An integrated circuit manufacturer uses its network to control production of custom chips. The production process includes preprogramming each chip with firmware designed for a specific customer. The firmware has passed all qualification testing and is under strict configuration control. As the final step in production, following final QA testing of IC devices, the manufacturer loads each device with customer-specific firmware from its configuration controlled source files. A virus infects the manufacturer's network, including the firmware source file. Each IC shipped is, in turn, infected by the virus. Customers install the virus-laden ICs in their own products. When the completed products are used by downstream customers, their networks are infected. The manufacturer's customer must recall and replace all infected products. In addition, the customer is liable for damage to downstream customers' networks. The manufacturer's customers sue, seeking recovery of their product recall and replacement cost, their cost to defend lawsuits filed by downstream customers, and damages awarded to downstream customers for damage to their networks.

**For more information about CNA, contact your local independent agent or visit www.cna.com.**