Cyber Insurance 101

Building Cyber Readiness and Resiliency

Andres Franzetti
Chief Strategy Officer
and Founding Member
Risk Cooperative

Andres Franzetti serves as Chief Strategy Officer and a founding member of Risk Cooperative, an innovative strategy and risk advisory firm based in Washington D.C. He is a fellow at the American Security Project, and recognized thought leader in the risk and cyber domain, having been most recently featured in Forbes and other leading publications.

The Need for Cyber Insurance

Cybersecurity is a growing concern for companies of all sizes, yet none may feel the impact more than small and medium-sized businesses (SMBs). SMBs are a core focus for cybercriminals as they are viewed as a soft target. The typical SMB lacks a rigorous cybersecurity defense and staff to deter a cyber-attack, let alone respond and recover from when when they occur. 62% of all cyber-attacks, roughly 4,000 a day, are targeted to SMBs according to a recent study by IBM. Larger organizations not only have the balance sheets to be able to withstand the costs of a cyber-attack, they also have a more robust cybersecurity team, investment strategy and technology approach to combat cyber-attacks. SMBs often do not have that level of organizational and financial resiliency. The U.S.' National Cyber Security Alliance found that 60% of SMBs that suffer a cyber-attack, are out of business within six months. When we look at the costs associated with clean up and remediation of a cyber hack, it becomes increasingly clear to see why this is the case. The average price for small businesses to clean up after a cyber-attack is approximately $690,000, with the figure rising to over $1 million for middle market firms[1]. The stark reality is the organizations in this segment of the market do not have the funds on hand to pay for a cyber-attack and keep operations going. The growing specter of ransomware attacks, like the WannaCry exploit, which reached 150 countries over a weekend, underscore the vulnerability to sophisticated cyber-attacks.

Cyber insurance is one way to help SMBs improve their defenses. A cyber insurance policy provides several benefits to these organizations:

- Reduces the financial liability associated with a cyber-attack.
- Provides additional breach response resources in the event of a cyber-attack.
- Provides additional assessments and guidance on how to develop a more robust cybersecurity framework.
- Provides compliance and breach notification support following an event.

There are several types of cyber insurance programs on the market today. The majority of organizations tend to opt for what is most often a bundled policy. A bundled policy means that cyber coverage is bolted onto an insurance policy the company is already purchasing, such as Business Owners Policies, Professional Liability, or a Technology E&O policy for example. These types of policies need to be evaluated very carefully to make certain they are providing the right level of protection. The other type of cyber insurance, and the one that is recommended, is a standalone cyber insurance policy. This policy is designed to specifically address the risks associated with cyber insurance, and carries a broader level of protection for the company purchasing coverage.

1 Ponemon Institute

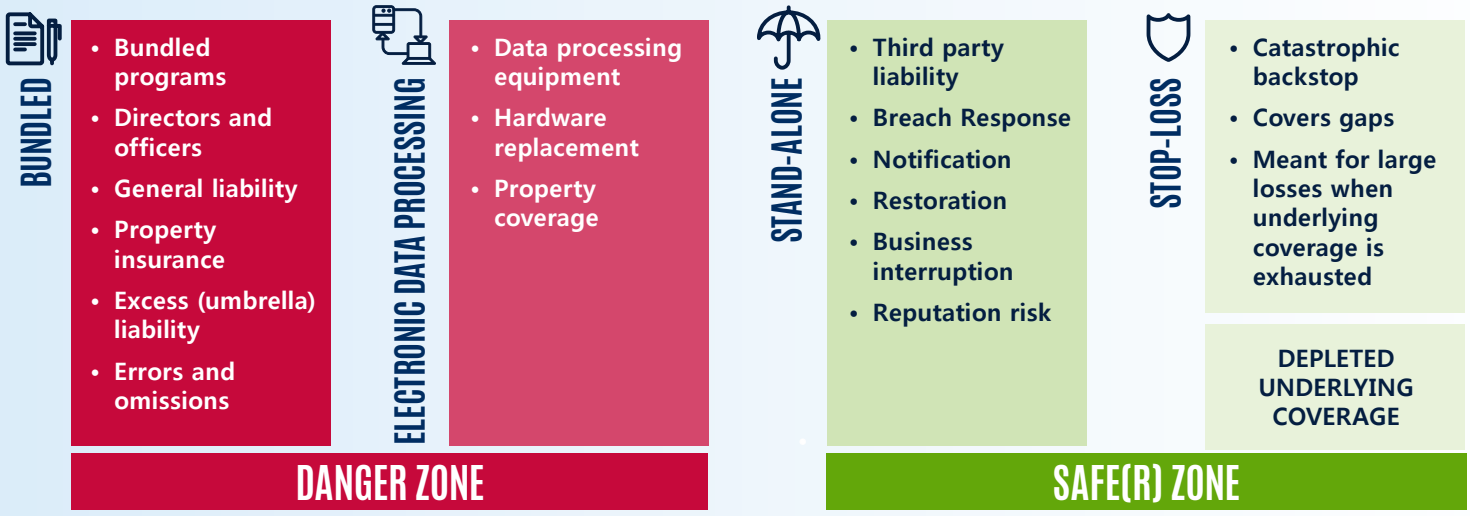
AMERICA'S SBDC FLORIDA

→ FloridaSBDC.org

floridasbdc.org/cybersecurity

Helping Businesses Grow & Succeed

Bundled products, especially with a risk that has such far reaching implications like cyber does, can become a source of confusion, especially during a cyber insurance claim, as to which policy and area of coverage should respond. This can lead to costly litigation, finger pointing among insurers and uncovered losses. The following diagram helps to highlight some of the most common policy types and recommendations.



Cyber insurance is not a coverage area that can be effectively sold without an experienced specialist to help guide customers through all the necessary exposures and potential coverage gaps. Seeking out a cyber risk professional to walk through the various components of a cyber policy is best to ensure you are adequately covered.

Key Coverage Checklist

The following outlines the key coverage areas of a cyber insurance policy, and the specific jargon that should be taken into consideration.

Third Party Coverage

- ☐ Build cybersecurity procedures in concert with business partners so that they have appropriate protections in place for your shared information.
- ☐ Consider cybersecurity as part of your contractual agreement with business partners and conduct regular risk assessments.
- ☐ Define requirements for data security and ensure that information is secured in all areas it is transmitted.

First Party Coverage

- ☐ **Theft and Fraud**
  Does the policy provide cover for costs of theft or destruction of data and theft of funds?
- ☐ **Forensic Investigation**
  Does the policy cover the costs of investigating to determine the cause of a loss of data?
- ☐ **Network/Business Interruption**
  Is coverage provided for business continuity and recovery expenses following a cyber-attack or breach?
- ☐ **Extortion/Cyber-terrorism/Ransomware**
  Does the policy provide coverage for the costs of "ransom" if a third party demands payment to refrain from publicly disclosing or causing damage with confidential electronic data, or taking control of files and servers?
- ☐ **Data Loss and Restoration**
  Does the policy offer protection to cover the costs of restoring data if it is lost, as well as diagnosing and repairing the cause of the loss?

→ FloridaSBDC.org

Helping Businesses Grow & Succeed