

Cybercrime is on the Rise among Financial Service Professionals. **Are You Exposed?**

A decade ago, criminals used guns. Today, all they need is a computer. With all the sensitive customer data you store, financial service professionals provide a target rich environment for cybercriminals. They steal tax returns, social security numbers and other personally identifiable data to sell on the black market – and they do it all the time.



Cybercriminals use Advanced Technology, including:

- Automated artificial intelligence software to randomly search for vulnerabilities
- Phishing attacks to infiltrate your systems and plant malware that monitors your activities
- Ransomware attacks that lock you out of your files until a payoff is paid in bitcoins
- Fraudulent impersonation schemes to trick unsuspecting employees to wire transfer them funds



Financial Service Firm Cybercrime Statistics

- Cyberattacks cost financial service firms more to address than any other industry²
- The average number of breaches per firm has more than tripled over the past five years²
- The average cost of a data breach per firm has increased by 40% over the past three years²
- \$148: Average cost per stolen record of a data breach³
- 50% of all email is spam, and 73% of all spam is malicious³
- 206 days: Average number of days it takes to identify a breach³
- \$133,000: Average cost of a ransomware attack on small businesses³

How exposed is your business?



Get a **FREE** cyber risk assessment with recommendations to help reduce your risk.

See what a hacker sees. Externally observable data is used to help protect your small business. No downloads, software, or agents required.

- Receive clear, actionable steps to help reduce your business' cyber risk
- Discover exposed usernames, passwords and personally identifying information
- Find exploitable vulnerabilities and misconfigurations that expose your business to cyber threats



Basic actions like a cybersecurity assessment can help reduce your exposure by 80%.⁴

For a free cyber risk assessment, please visit: aoncyberEZ.com

To help protect your business from attack you must stay one step ahead of cybercriminals

Introducing Sophisticated, Comprehensive Cyber Liability Insurance



CyberSecurity Platform

- Threat Monitor** – Constant monitoring for new risks, alerting you before damage is done
- 24/7/365 Helpline** – A dedicated team of cybersecurity experts are available to you at all times
- Credential Monitor** – Receive an alert when your logins and data have been compromised
- Ransomware Prevention** – Software protection against 99% of known ransomware
- Patch Manager** – Continuous scanning of your systems for out-of-date software and vulnerabilities



3rd Party Liability Coverages

- Network & Information Security Liability:** Up to \$15M in liability damages, plus the costs to defend you
- Regulatory Defense & Penalties:** Includes coverage for state and federal regulatory fines & penalties
- Multimedia Content Liability:** Covers multimedia wrongful acts such as infringement, piracy, etc.
- PCI Fines & Assessments:** Covers fines resulting from a failure of your security, data breach or privacy violation
- Bodily Injury & Property Damage:** Pays for defense and damages when a security failure results in physical harm
- Technology Errors & Omissions:** Coverage when your technology service or product is the cause of loss



1st Party Liability Coverages

- Fund Transfer Fraud:** Pays for funds transfer losses you incur from security failures or social engineering
- Cyber Extortion:** Covers the costs to respond to a ransomware incident, even including virtual currencies paid
- Computer Replacement:** Pays the cost to replace your computer systems that are permanently impacted
- Business Interruption & Extra Expenses:** Covers financial losses and expenses incurred after a data breach
- Data Privacy Expenses:** Includes client notification costs, credit monitoring, forensics, PR and more
- Digital Asset Restoration:** Replace, restore, or recreate damaged or lost digital assets

Worldwide Coverage: Protect your data and assets anywhere in the world

Cyber Terrorism: Each policy includes protection from acts of cyber terrorism

Internet of Things: Coverage for all of your IoT devices is included by default

Social Media: Coverage for your social media accounts is included by default

For a free cyber risk assessment and to apply for coverage,
please visit: aoncyberEZ.com

Brought to you by:



Powered by:



¹"99 Inspiring Cybersecurity Quotes," Pingleton, August 31, 2019.

²Chris Thompson, "What's the cost of cyber crime to your company and how should you respond?" Accenture, June 25, 2018.

³Rob Sobers, "110 Must-Know Cybersecurity Statistics for 2020," Varonis, April 15, 2020.

⁴29 Must-know Cybersecurity Statistics for 2020, Cyber Observer, 2020.

Aon CyberBusinessProSM is a service mark of Aon Corporation. Coalition, Inc. is the exclusive administrator.

This document provides summary information only. Insurance coverage is subject to specific terms, limitations and exclusions, and may not be available in all states.

EZ Insurance Solutions is the brand name for the brokerage and program administration operations of Affinity Insurance Services, Inc. a licensed producer in all states (TX 13695); (AR 100106022); in CA & MN, AIS Affinity Insurance Agency, Inc. (CA 0795465); in OK, AIS Affinity Insurance Services Inc.; in CA, Aon Affinity Insurance Services, Inc., (CA 0G94493), Aon Direct Insurance Administrators and Berkely Insurance Agency and in NY, AIS Affinity Insurance Agency.

© 2020 Affinity Insurance Services, Inc.