Getting the Most from Cyber Insurance

cyber security data privacy

Summary: Cyber insurance can be part of protecting against digital crime. We discuss how it can protect financial institutions and their customers against financial losses and provide other resources if and when a cyberattack occurs.

One of the biggest data breaches of 2022 caused the release of over 1.2MM credit card numbers over the dark web, which included the credit card holders' names, social security numbers, email addresses, and more. The site responsible, called BidenCash, allegedly stole the information through malware and e-commerce hacking, proving how vulnerable many businesses still are to cyberattacks.

The statistics on cybercrime are staggering. Around 53.35MM Americans were victims of cybercrime in the first half of 2022, with the US comprising nearly half of all global cybercrime. Americans lost $6.9B to cybercrime in 2021 that included scams involving romance, investment, and business email theft. Undoing the damage of ransomware attacks cost an average of $1.08MM in 2021 and $2.09MM in 2020.

Only half of US organizations have full cyber insurance coverage; another 28% have partial coverage. About 12% of American organizations have no cyber insurance coverage at all.

Community financial institutions (CFIs) can play a part in protecting themselves and their clients from cyberattacks. Regulations require CFIs to have cyber coverage, although the coverage amount is up to them. CFIs are also in a perfect position to advise business customers on cyber coverage: why it's worth getting, and how to make the most of whatever insurance they select.

Small businesses are ideal targets.

When small-business owners see huge targets such as Microsoft and the Red Cross get hit by cyber bandits, they might think that smaller companies such as themselves are safe. However, no business is too small to experience a data breach from a cyberattack. *"A lot of people have this notion that it will never happen to my business or my bank, because it's too small,"* says Linda Comerford, assistant vice president of incident response and cyber services at AmTrust Financial Services Inc. *"You actually see more instances of issues with the smaller businesses."* For instance, Comerford says, her firm worked with a CFI that had to close for two weeks because of a ransomware attack. The CFI could not reopen until they paid a negotiated ransom.

Rather than looking at size, cybercriminals key in on vulnerabilities they can exploit, and smaller organizations tend to have more of these. CFIs may have some of these vulnerabilities as well, which is why it's just as important for CFIs to assess their current cyber insurance coverage as it is to encourage customers to take out a cyber insurance policy of their own.

Without a cyber insurance policy, an attack on a smaller organization could have devastating consequences. Security Magazine reports that, of businesses with fewer than 1K employees, 67% have had cyberattacks that cost firms an average of $200K per incident. About 60% of companies that were forced to halt operations never opened for business again. On the customer side, an attack could mean a client losing their business, but for a CFI to experience damages beyond the scope of their own policy would be just as detrimental to the customers who could temporarily lose access to their accounts.

How much cyber insurance is needed?

Cyber insurance varies between carriers and individual policies. Along with first-party coverage that would pay for damages to your CFI or the insured business, a policy might also include third-party insurance, which covers harm that's come to your CFI's clients or a business' vendors as a result of a cyberattack. For instance, if a cyberattack on a CFI left one of its clients unable to do business without data restoration, third-party insurance would pay the cost of the data restoration and business interruption.

In practical terms, first-party insurance on a business or a CFI might pay for the cost of forensics and analytics to discover the extent of the damage, ransom, business interruption, data restoration, and notifications to employees and clients, plus attorney fees.

Liability coverage might also be part of first-party insurance, especially as general liability insurance doesn't typically include cybercrimes in its coverage. This insurance would help pay the costs of lawsuits, regulatory action, and fines that might proceed from a cyberattack.

As always with insurance, figuring out how much coverage you and your business customers need involves assigning a value to what you want to protect. In the case of your CFI, you'll also want to consider the measures you've already taken to keep your CFI and your business customers safe from cyber predators. Your CFI may have a lot of protections in place due to the sensitivity of information your staff handles, and coverage should reflect that. However, a smaller business may not believe they need much protection, and thus could have little to no security in place. The policy chosen for a CFI or a business should be appropriate for the types and levels of risk you have, the potential costs of those risks, and the security and precautions you have available to protect your data. You'll also want to have a team to analyze and select the appropriate coverage.

Take advantage of insurance resources.

One of the best ways cyber insurance can help CFIs and their small business customers is by providing access to experts who can direct the response to a cyberattack, mitigate the crime, or respond to the crime.

Information about proactive things a CFI can do to protect itself from cyberattacks is perhaps an even better use of access to experts. Some insurance companies even offer discounts to businesses that have deliberately made themselves less attractive targets.

As it's said, the best insurance is the insurance you never need. That's particularly true of cyber insurance. Although coverage claims can be knotty and complex, leaving your CFI and your small business customers vulnerable to hacks and breaches is worse. A combination of coverage and careful attention toward protective measures can be a sweet spot for you and your clients.

NEED MORE FEE INCOME?

Financial institutions can earn additional fee income by adding monetization to a hedged loan. Learn more about how Borrower's Loan Protection® (BLP) can help you earn higher fee income today.

ECONOMY & RATES

Rates As Of: 02/13/2023 05:34AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	4.79	0.09	0.37

6M	4.89	0.09	0.13
1Y	4.87	0.20	0.16
2Y	4.54	0.34	0.11
5Y	3.94	0.33	-0.06
10Y	3.75	0.24	-0.13
30Y	3.81	0.18	-0.16

FF Market	**FF Disc**	**IORB**
4.57	4.75	4.65

SOFR	**Prime**	**OBFR**
4.55	7.75	4.57

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.