“Insuring” Cyber Success For SMBs

cyber security business customers ransomware

Summary: With the recent cyberattack on Kaseya, cyber concerns remain high among many businesses, especially small businesses. For good reason, as 43% of cyberattacks target small businesses. Community financial institutions may want to familiarize themselves with cyber insurance basics to help guide their business customers as more may turn to insurance to protect themselves. We provide four cyber insurance considerations.

Did you know that Alektoraphobics are extremely afraid of chickens? While only 9% of the US population have this phobia, it can be intense for those that suffer from it, as just the thought of a chicken can trigger this fear.

There are many things to fear out there, but right now, cyberattacks are high on the list for many bankers and businesses. The myriad recent mega cyberattacks, like those on the Colonial Pipeline and more recently Kaseya, have caused huge, far-reaching ripple effects on critical infrastructure and impacted millions of people. Not only that, but cybercriminals are also moving downstream.

While not as widely reported, threats to small and mid-businesses (SMBs) and community financial institutions (CFIs) are on the rise too. Less-experienced cybercriminals are working from basic, off-the-shelf scripts that they have acquired through the dark web. They perpetrate their own ransomware attacks, data thefts, and other intrusions. The thinking is that smaller organizations are often less prepared for such attacks — lacking the resources of larger business and bank counterparts to spend on technological protections and cyber-hygiene education for employees.

Indeed, according to Purplesec, a cybersecurity company, 43% of cyberattacks take aim at small businesses, with 70% of these businesses not prepared for such attacks. Not only that, but it’s also projected that small businesses experience a ransomware attack every 14 seconds. The impact of these cyberattacks has forced six out of 10 SMBs to close within half a dozen months after the attack, suffering from financial losses.

Hence, SMBs are more actively considering and investing in cyber insurance (or cyber liability insurance) to indemnify them and offer financial protection in the case of losses from online attacks. (Until the pandemic cyber-spike, 83% of small businesses did not carry this liability insurance.) But before CFIs choose to recommend or offer cyber insurance to their valued business customers, bankers may want to familiarize themselves with some of the basics of these policies, including what they may offer and what they may not. Here are some considerations to start with.

1. **Watch the exclusions.** Exclusions can severely limit the claims that might get paid. As with all insurance policies, exclusions apply to cyber liability. As a rule, the lower the premiums, the more exclusions are typically included. Exclusions might rule out claims related to employee error, software that has not been properly patched, hardware that is considered too old, breaches initiated through a third party, or other specific situations. It is vital to understand upfront what incidents may not be covered to avoid high costs and lawsuits down the road.
2. **Meet the specific policy demands.** The business’ systems and protocols must meet the demands of the policy. Cyber insurance policies are evolving on a continuing basis, as they are embraced by more

companies and financial institutions. To be accessible to smaller organizations that may not want to pay hefty premiums, many of these policies require that the business meets certain standards of updating their systems, maintaining redundant files (especially in the case of ransomware threats), and offering adequate cyber-hygiene education to employees. In the event that a business falls prey to a breach and it has not met the required standards, the policy might be voided.

3. **Confirm employee error is covered.** It's often pointed out by cyber experts that the biggest security threat is the person between the chair and the keyboard (i.e., the human factor). Undeniably, bad actors are increasingly using social engineering ploys to gain access to systems or get unsuspecting employees to release funds or data to them directly. Forty-three percent of small business cyberattacks were through phishing/social engineering, according to Purplesec. While some cyber insurance policies include so-called "social engineering endorsements," not all do.
4. **Check on third-party intrusion coverage.** Ask if intrusions initiated through third-party vendors are included in the plan. Some of the most infamous cyber breaches (i.e., Target, et al) began with cybercriminals finding access through a third-party vendor, not the organization that ultimately suffered losses. Insurers are aware of this and also aware that even SMBs are often supported by a wide network of outside providers. Depending on the policy, access through "preapproved" vendors to the business may be covered, especially if the vendor can show that they have their own cybersecurity house in order.

OUTSOURCE ALM SERVICES AND REST EASY

Regulators have raised the bar on interest rate risk and liquidity analysis. We can help you effectively manage your ALM and give you back some preciously needed time. To see how easy it can be & get expert help, contact us today.

ECONOMY & RATES

Rates As Of: 07/19/2021 02:53PM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.05	0.00	-0.04
6M	0.06	0.00	-0.03
1Y	0.08	0.00	-0.03
2Y	0.23	-0.03	0.10
5Y	0.71	-0.18	0.35
10Y	1.20	-0.28	0.28
30Y	1.82	-0.27	0.18
FF Market	**FF Disc**		**IORB**
0.10	0.25		0.15
SOFR	**Prime**		**OBFR**
0.05	3.25		0.08