SAYATA

SMBs are struggling to get cyber insurance;

Here's how to stay protected.

POLSINELLI

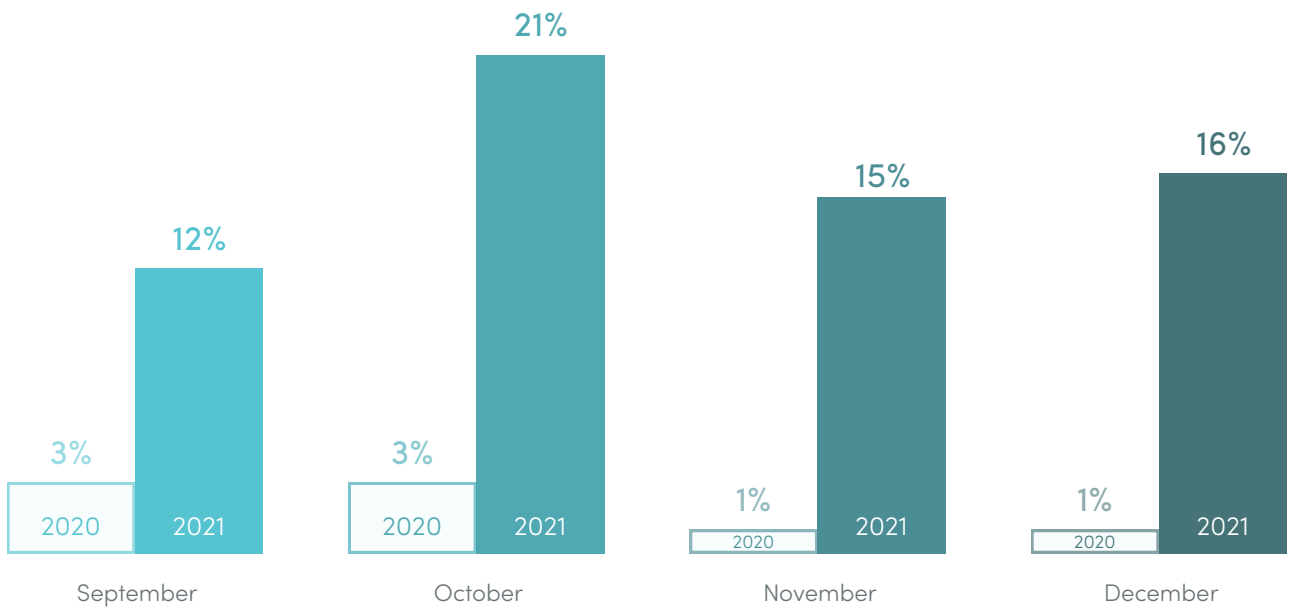
SMBs are struggling to get cyber insurance; here's how to stay protected

For the first time ever, cyber insurance is facing a hard market. Since the product line's inception about twenty years ago, carriers, brokers, and policyholders have reaped the benefits of soft market conditions. Policies were cheap, and they provided generous coverage and low retentions. Losses were minimal, and therefore, cyber insurance books were very profitable.

Over the last few years, the cyber risk landscape has shifted. The frequency and severity of losses has grown astronomically, forcing carriers to constrict their offerings and raise premiums. Agents and wholesalers are feeling squeezed as insureds are looking for more coverage options, greater understanding of coverage, and competitive rates.

Cyber pricing is on the rise in a big way

Percentage of Cyber Accounts with Greater than 100% Pricing Increase



* According to Cyber REDY® Index 2021

Why are we in a hard market?

When carriers began selling cyber insurance, the risks facing large companies were one-off incidents like lost unencrypted laptops, misfired emails with lists of employee information, and the occasional malicious insider. Smaller companies had even fewer issues. Over time the threats evolved and grew to include more email compromises and small ransomware interruptions. But even those could be resolved quickly by restoring from backups and resetting passwords.

However, in the last few years, the attack landscape has transformed significantly. Companies of all sizes started experiencing significant email compromise events that very often involved the expensive combination of large-scale data breach investigation and notification, and the loss of funds through misdirected wire transfers or ACH payments. Phishing and social engineering campaigns exposed a lack of employee training, technical safeguards, and data retention policies across many companies. Each of these incidents may cost tens of thousands of dollars to resolve on average, and the frequency led to huge loss ratios for cyber carriers.

Further, small companies were not immune to these issues, and the costs associated with the investigations and response compared to the premiums paid for the policies exposed the small business space.

Just as carriers and brokers seemed to wrap their arms around business email compromises, by pushing extensive training and technical solutions, ransomware events exploded much larger than ever anticipated. Early on, ransomware was typically used to encrypt data in place. Attackers would access a network, quickly encrypt what they could, and demand a few hundred or a few thousand dollars in exchange for a decryption key.

But as attackers saw companies responding rather successfully to these events, they shifted the nature of their attacks. Instead of simply locking users out of a network the moment access was acquired, attackers instead saw the potential for larger pay days with some additional effort. They sat stealthily in a network performing reconnaissance to understand the company's backup strategy and to steal important company data, ultimately using internal phishing campaigns to escalate user privileges to gain access to critical systems.

Once sufficient network administrator level access was obtained, the ransomware attack was launched, finally encrypting the network a few days or months later. When these types of attacks hit companies, they were not only dealing with an overwhelming hit to critical systems and data and backups being encrypted, but also the added concern of data being accessed or stolen, and potentially exposed. This allowed attackers to demand much higher ransom payments—to the tune of millions of dollars per event.

Between the business interruption, extortion demand, data restoration, and incident response, policies with $5 million or $10 million in coverage that had never been touched were exhausted on a weekly basis. Further, unlike a typical data breach matter, ransomware matters are immediately public events. Public events like this draw attention from regulators and class action attorneys, especially when downstream services to customers are interrupted as a result.

What does that mean for the market?

> What we had seen prior to 2019/2020 was an environment where it seemed like you almost couldn't lose money, and cyber insurance trends only ran in one direction – towards lower rates and broader coverage.
>
> It's a very different story today. What we see now, and what we've seen for the last year or so, is an environment in which carriers across the board are **taking rate – sometimes double - or triple-digit rate increases depending on the segment of the market**. That rapid expansion of coverage driven by competition in the marketplace, has really slowed down quite a bit.

Tim Zeilman
Global cyber product owner,
at HSB, a Munich Re company

Carriers have responded to the new landscape by increasing premiums, decreasing policy limits, and being more conservative in their underwriting process. Where it was previously hard to convince certain markets with minimal data collection and personally identifiable information that cyber insurance is essential for business, the demand for policies in those markets now outsizes supply.

At renewal, carriers have updated application questions, often times with assistance from forensic experts, to better understand a company's preparation for ransomware attacks and the subsequent business interruption. Carriers are now requiring additional technical safeguards, like multi-factor authentication (MFA) and endpoint detection and response tools (EDR), where previously organizations that implemented these tools were considered leagues ahead of their peers.

The sudden shift towards requiring these protections as a prerequisite for coverage has left many organizations scrambling to find time and money in their IT budgets to implement these services ahead of a policy renewal.

In addition to increased premiums, limited coverages, and higher security expectations, many carriers are outright declining risks in certain markets that have proven to be susceptible to expensive attacks. Manufacturing, technology supply chain providers, and healthcare institutions have especially faced an uphill battle in finding carriers willing to underwrite their businesses. This forces those organizations to purchase more expensive policies with lower coverage and build more complex towers of insurance in order to maintain the amount of risk protection enjoyed for many years prior.

What can be done?

Carriers are expecting organizations to have basic modern IT security controls and data protection policies in place, and to be able to demonstrate that they are implemented correctly and enforced constantly.

01 Effective Backup Strategy, and Testing

A big reason ransomware has exploded so successfully is that attackers have taken away a company's option to restore without paying the ransom by either encrypting or deleting backups as part of the initial attack. In response, many forensic experts recommend the "3-2-1" approach—3 copies of the data (production, on-site backups, off-site backups), 2 different media types (cloud, disk, snapshot, or tape), and 1 offsite copy (cloud, tapes).

When it comes to ransomware, best laid plans often go awry. All too often an organization implements what they believe is a sound strategy, only to find out during an attack that their backups were not segregated properly, or the daily snapshot stopped functioning months ago. Carriers expect organizations to be able to demonstrate a regular testing schedule and the results of those tests.

These tests will enable organizations to better anticipate potential downtime, restoration strategy and prioritization.

02 Multi-factor Authentication (MFA)

Most ransomware attacks start with an account takeover. Once credentials are stolen, attackers typically use credential-harvesting malware to escalate privileges in order to gain access to a network administrator account. Companies that properly implement MFA across all users can thwart many of these attacks. Rather than just asking for a username and password, MFA requires one or more additional forms of verification (like a one-time use code sent to a user's phone), which decreases the likelihood of an attacker gaining access to the account.

MFA should be implemented on all email accounts, local administrator accounts and domain administrator accounts, and on any remote access points. If you work with third party vendors who have direct access to perform some function on your network, MFA should also be enabled here too.

03 Data Retention Policies

As mentioned above, ransomware attacks have shifted from encryption only, to encryption + data access. While much of this article is focused on the business interruption and data restoration issues caused by ransomware attacks, the access and acquisition of sensitive data is another hurdle organization must overcome. For organizations that can restore from backups and avoid a huge interruption, they still must consider the data breach implications of the stolen data. Most often, attackers will provide a sampling of stolen data at the outset of a conversation with the victim organization, in order to encourage payment for the return and destruction of the information.

What can be done? (continue)

Organizations that have strong data retention policies and enforce those policies limit the amount of extraneous data available for attackers to monetize. They can also use the sampling to pinpoint where on the network the attacker may have stolen the data from, in order to get a better sense of what they might have and to better focus a forensic investigation.

Further, for the ongoing issue of business email compromises, inbox hygiene and email archiving drastically limit the data potentially available in a compromised inbox, substantially decreasing the time and money spent determining what the attacker could have had access to while in the compromised account.

04 Endpoint Detection & Response (EDR)

EDR is a next level antivirus solution. It not only provides real-time monitoring of your endpoints for any anomalous activity, but it can also quickly alert security personnel to security issues, allowing organizations to contain an incident before it becomes catastrophic. Further, when an incident does occur, forensic investigators can use the EDR logging to understand the timeline of the attack and any movement that occurred in the network.

This can speed up the response and help an organization understand what, if any, data is at risk as a result of the limited intrusion.
However, EDR is only as good as the monitoring of alerts. Because attackers tend to strike at inopportune times, it is important to have dedicated resources to rule out false positives from legitimate threats. There are many 24/7 security companies that offer these services.

How can brokers help?

Brokers are keenly positioned in the ecosystem to ensure that organizations seeking coverage are optimally informed and prepared. Here's how:

A

Brokers help insureds meet carrier requirements - Brokers can help insureds navigate increasingly stringent carrier expectations and adapt to them. Having access to applications across the market, brokers are in the best position to educate and prepare clients for the inevitable squeeze. Because many of the required safeguards need additional IT financing and company buy in, brokers can help clients by flagging issues they need to be prepared for earlier in the application process. "Cyber wholesalers are in a particularly unique space, acting in concert with their agency partners to constantly educate insureds on the ever-changing cyber threatscape and how to adapt security controls to it. Cyber brokers are on the front lines of the frequent changes in underwriting and how these translate to real-life adjustments that small businesses have to make to their cyber hygiene," said Diane Templin, Director of Insurance Operations at FifthWall Brokerage.

B

In line with that, through their connections to the legal and forensic fields, brokers also help insureds by putting them in touch with resources that can assist them in identifying gaps in their current cybersecurity posture and remediate those gaps prior to the application process. Templin added, "Often brokers, work directly with a business's law firm and IT department, or MSP, to communicate the needs of carriers so the business can get coverage as well as stay protected."This includes specifics like conducting privileged risk assessments, penetration tests, and gap analyses and then implement solutions based on the results of those activities.

C

Brokers know their client's business and understand what coverage they need - Brokers are in the unique position of understanding the insured's cyber posture (as per above) and their business needs. As cyber coverage constantly changes to adapt to the ever-changing threatscape, brokers are keeping a pulse on product updates from carriers, allowing them to recommend the best, most relevant coverage for the insured.

D

Once the insured adjusts their cyber posture to align with carrier guidelines and coverage needs are identified, brokers have vision into the market options and can shop and secure competitive coverage and rates for new and renewal policies.

Authors:

- Pavel Sternberg,
  Partner at Polsinelli LLP
- Caitlin Smith,
  Technology Transactions & Data Privacy Associate at Polsinelli
- Asaf Lifshitz,
  CEO at Sayata

SAYATA

POLSINELLI