ZELDIS THOUGHT LEADERSHIP

Cyber Risk Reality: Small Business Attitudes Toward Data Security Threats and Cyber Liability Insurance

ZELDIS RESEARCH ASSOCIATES

OCTOBER 2024

Our Methodology

Webcam IDIs

N = 13 total

1 hour each

September 12 – October 1, 2024

Ages: 5 Millennial, 6 Gen X, 2 Boomer

Gender: 7 Female, 6 Male

Business Types include:

- Retail, business services, consulting, healthcare, nonprofit, construction,, restaurants

Recruiting

- Own or run a small business, sole proprietor to 100 employees
- Have at least one line of business insurance (e.g., GL, Property, BOP)

Have cyber liability: 9

Do not have cyber liability: 4

“I’m just a small business owner. Why should I care about cyber risk?”

Small businesses are vulnerable….

"46% of all cyber breaches impact businesses with fewer than 1,000 employees."

(Source: 35 Alarming Small Business Cybersecurity Statistics for 2024 - StrongDM*)*

"Nearly 50% of small businesses that experienced a breach took weeks or longer to discover it…Most insurers do not provide an all-inclusive policy that will cover all of the expenses associated with a data breach."

(Source: Data Breach Insurance: What It Is, Which Businesses Need It - NerdWallet*)*

"On average, small businesses spend between $826 and $653,587 on cybersecurity incidents…The next five years are due to see a 15% increase in cybercrime costs, reaching 10.5 trillion by 2025."

(Source: 51 Small Business Cyber Attack Statistics 2024 (And What You Can Do About Them) - Astra*)*

Awareness and Attitudes

How do SBOs approach cyber risk?

Small businesses touch a wide variety of data.

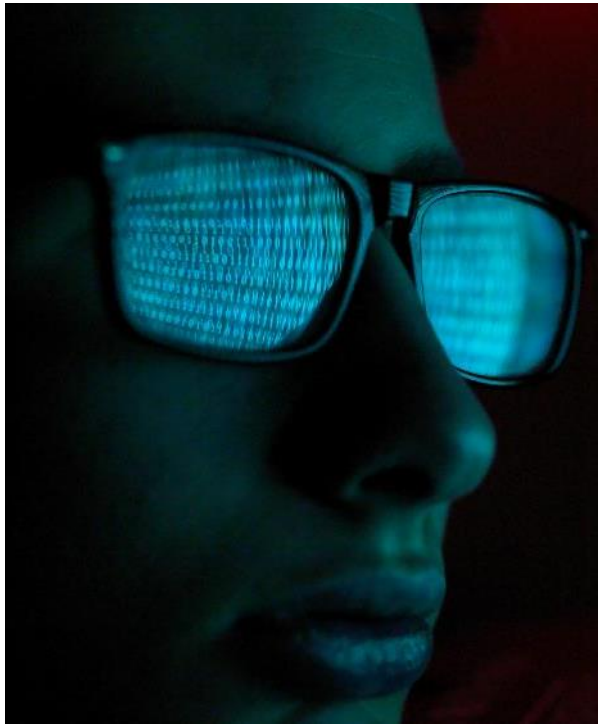
They have some concerns about data they keep internally, but also worry about third-party vendors, especially businesses who use point of sale systems and/or process credit cards.

Customer Data | Employee Data | Financial Data | Proprietary Data | Medical Data

"We have proprietary information. What is ***worrisome is third-parties that hold data of their customers****. It's really important to watch their potential data breaches because of credit cards.* ***Toast has information of all employees****. That is a huge responsibility." (SBO Without Cyber Liability)*

They are hearing more about cyber threats, especially over the past few years.

Many have heard about data breaches and cyber losses, often in their personal/consumer life. More established businesses are more likely to network with other SBOs and hear about their experiences.



- Phishing
- Hacking
- Spoofing (email, voice/image fraud)
- Wire transfer fraud/false invoices
- Client information leaks
- Vendor data breaches
- Employee errors / ex-employee retaliation

"If it happens to AT&T, it could happen to you."
(SBO With Cyber Liability)

*"Hearing more about **breaches from massive companies like Equifax** and having those **close calls within our own business**. It just started to make sense that this is a risk. It's **very possible that we'll have an issue at some point** and who knows how expensive it could be." (SBO With Cyber Liability)*

Some have even had incidents themselves, personally or professionally.

PROBLEM

SOLUTION

Accountant sent money to hacker	MFA set up and new cyber policy
More than one “close call”	Purchased cyber insurance
Mom was the target of an attack	Cyber security reminders

*“We hadn't had MFA set up yet. **The organization got hit pretty hard.** They got into an email account and sent some **fake emails** with and ended up **getting our accountant to send quite a bit of money**.” (SBO With Cyber Liability)*

*“The attack on my mom was affirmation that we need to **continue to be diligent** when it comes to online activity. I don't think it was an epiphany where I said, ‘we need to overhaul everything that we're doing.’ But **it was certainly a reminder.”** (SBO With Cyber Liability)*

However, some still think of themselves as too small to be a significant target.

SBOs' main priorities are running their business and serving their customers. They don't want to spend time worrying, so many simply don't.

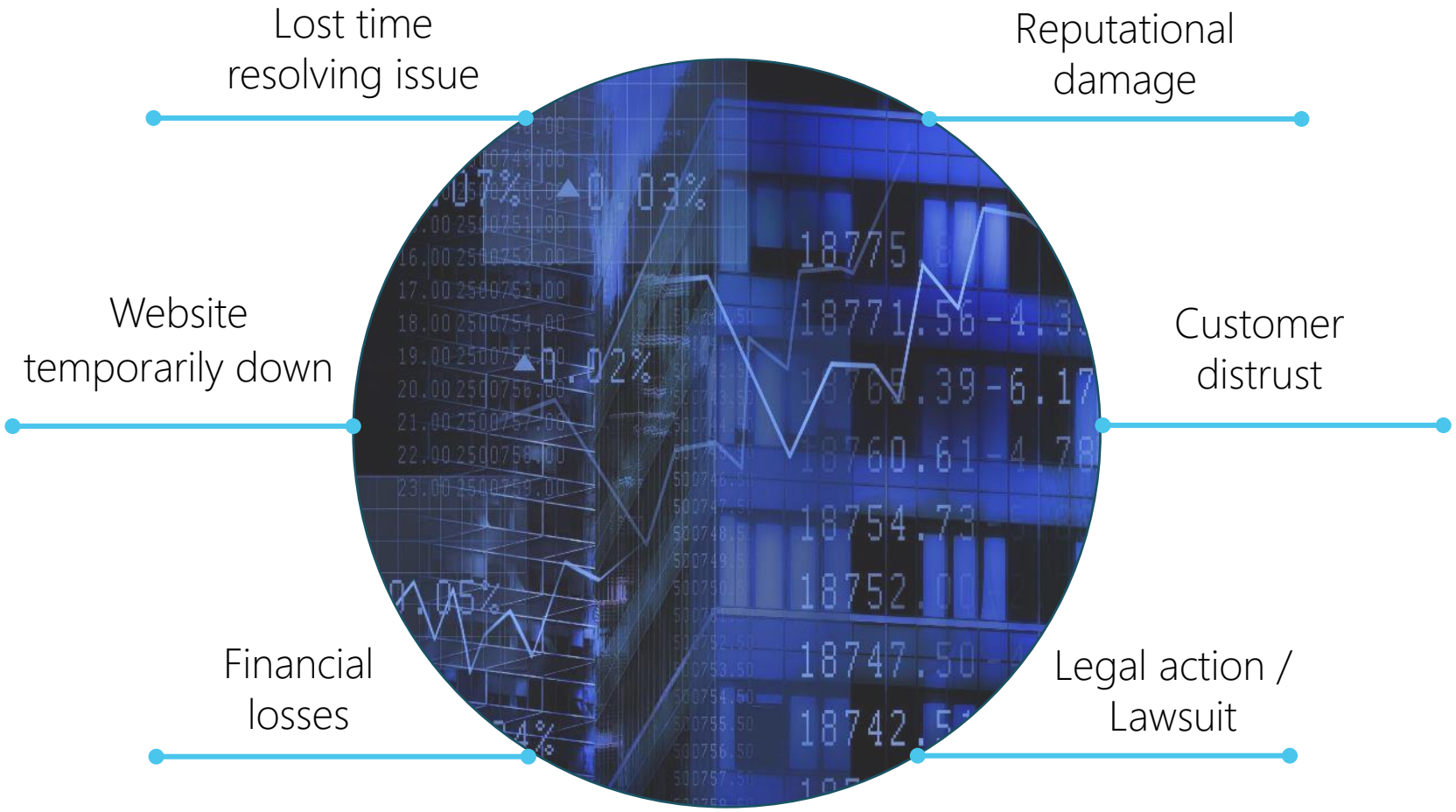
They tell themselves:

- **They're doing the best they can** with the resources they have; a cyber incident may be unavoidable, but they hope it will not dramatically impact their business
- **They aren't as vulnerable** as other types of companies, especially those who do not hold much customer data or who don't process credit cards
- They are **too small to be of interest** to hackers
- They are **too busy with their day-to-day,** and do not want to add to their stress.

*"I'm **not worried about it.** I've invested zero time. I have **not heard any of my friends** talk about problems with a breach." (SBO Without Cyber Liability)*

*"We could have an attack on the website [for e-commerce], but that would be rather surprising. **There's no money to be gotten**." (SBO With Cyber Liability)*

SBOs know the potential consequences of a cyber incident, but some are optimistic that customers would be understanding.



"We process payments online, take appointments online, we sell online. ***Everything we do is online.*** *If that got shut down or website was compromised,* ***it could be disastrous.*** *If we ever compromise their own personal information, that would cause a lot of issues and potentially* ***customers to lose trust****." (SBO With Cyber Liability)*

*"****People understand that it happens*** *and there's nothing you did or could have done to stop it. There're just bad people." (SBO with Cyber Liability)*

Protecting Themselves

What are small businesses doing to prevent cyber losses?

SBOs feel they have come a long way in addressing cyber exposures.

Relying on professionals:

- Several have in-house IT staff
- Others work with outsourced MSPs

Software and vendors:

- Using secure software and trustworthy providers
- Cloud storage
- Relying on third-party vendors' security
- Firewalls, anti-virus software

Procedures and training

- Multi-factor authentication
- Password rules and managers
- Single sign-on services
- Training staff (though largely informally)

*"We really **just rely on our IT** department to keep us out of trouble." (SBO With Cyber Liability)*

*"Our **software is cloud-based** so we've got the protection. I **assume my software company** has got their I's dotted and T's crossed." (SBO Without Cyber Liability)*

*"I have very **long, complicated passwords** and use a password manager. I have **limited access for my employees**." (SBO With Cyber Liability)*

*"I have compliance **classes on what to do when you get a phishing email** or something." (SBO With Cyber Liability)*

Keeping up with cyber security protocols and costs is a challenge.

Key Pain Points

Knowing when to implement additional security procedures

- These can be cumbersome and time-consuming for employees and leadership
- Most do not have formal disaster recovery plans or written protocols; they are still "winging it" to some degree

Having to trust vendors and software providers

- While this reduces the burden on SBOs and provides some peace of mind, it also makes them vulnerable to someone else's mistake

Increasing cost

- Relying on third-party IT/MSPs is a major expense; some try to limit the calls they make
- Software, systems, and cyber liability all add up

"I definitely think about logging in, MFA, but I see the difficulty people have every single time they log in. Just the ***dichotomy between convenience and security****. You can't have both." (SBO with Cyber Liability)*

But the biggest challenge is the great unknown.

While they try not to worry too much, SBOs acknowledge that new cyber threats are emerging all the time, and it's nearly impossible to stay ahead of the game.

"The biggest ***unknown is what's the next way that bad actors*** *are going to try infiltrate or get information, things like that. Predicting the future really, just so we could be prepared, but I'm* ***hoping our IT people are doing that research****." (SBO With Cyber Liability)*

GenAI represents the next frontier of cyber threats, though SBOs are not sure what the risk is yet.

- Some are using ChatGPT and other AI tools, and simply trusting that they are safe – but they are not entirely sure.
- Others know that AI is being used to spoof voices and images in "next level" phishing scams.

"We use ChatGPT…I guess I ***don't really know if any of those are a cyber danger*** *at this point." (SBO With Cyber Liability)*

Cyber Liability Insurance

How do small business owners approach cyber liability?

Many of these SBOs say they have some form of cyber liability/data breach.

However, they are not fully aware of:

- Whether they have a standalone policy or an endorsement onto another line of insurance
- Their limits, or even what is covered

Cyber Liability Purchase Triggers

- **Agent recommendations:** Most rely on their agent/broker to help navigate insurance products. Those with standalone cyber often say their agent advised them to purchase it.
- **Experienced an incident:** Being "burned" by a phishing attack or ransomware is a painful, but powerful motivator
- **Desire for protection/More news about breaches:** Seeing the increase in cyber attacks made some look for some peace of mind, "just in case."
- **Contract requirements:** Client agreements/MSAs
- **Business startup:** A few included cyber in their initial business insurance purchase.

Reasons for purchasing cyber liability…

*"The reason I did opt for adding cyber insurance to my general liability is the **storage of credit card data.** I said **yes when working with the agent** because it was reasonably priced." (SBO with Cyber Liability)*

*"During renewal time, they talked about **getting new and exciting products** that they could **augment the policy or endorse the policy** with. We felt data breach worked a little bit better for the cost." (SBO With Cyber Liability)*

*"**Protecting us from what we don't know, honestly**. We don't know what's coming down the pike, and we can **do so much to protect ourselves and be smart,** but I feel like there's just so many people that are trying to do this stuff and infiltrate stuff that it's like you can't outsmart them all. At some point, **someone is going to get through, and so prepare for it.**"* (SBO With Cyber Liability)

Those without cyber liability have heard very little about it.

Reasons for not purchasing include:

- I don't really know what it is; my agent has never brought it up.
- It's too expensive, costs are going up.
- We haven't had (a significant) incident yet.
- I trust that my colleagues won't fall for a phishing scam.
- Our malware and antivirus software protect us enough.
- If there is a vulnerability, my IT team will catch it.
- I am too small to be of interest to anyone.
- No one I know in my industry has suffered from an attack.
- If there is a loss, our vendors will bear the cost.
- I don't trust insurance companies in general; I don't believe in insurance.

*"It has **not been on top of mind**, cybersecurity, because a **restaurant business is so hands-on. It's not like a fintech**. I don't know what our level of risk is in cybersecurity. I don't hold people's financial data." (SBO Without Cyber Liability)*

*"Cyber has to be clear. I would have to **have someone say very clearly what this covers** and what my risks are." (SBO Without Cyber Liability)*

*"I've **never heard of cybersecurity** insurance. Is it worth getting now?" (SBO Without Cyber Liability)*

Small businesses lean heavily on agents for cyber insurance expertise; they want to be 'hands off.'

Cyber Carrier Selection Factors

Agent Recommendation

Most SBOs use an agent to get quotes, and several say they simply went with their **agent's carrier recommendation.**

'One-Stop Shop'

Some prefer to **work with carriers who have their other lines already,** such as GL, BOP, or professional liability. This makes billing and contacting the carrier easier.

Carrier Reputation

Some prefer a "name-brand" carrier with **strong financial stability,** which increases trust in the ability to pay cyber claims.

Cost

A few say they looked for the **lowest cost,** or the best value (coverage for the price).

*"The fact that **we have other insurance with Chubb made it easier**. The premium check is **just one check** we send out. They're a big **company and pretty secure**." (SBO with Cyber Liability)*

*"I **don't do any research.** I just **call my agent**. He is really knowledgeable. They send over the best one, **whatever is the most coverage at the least price**." (SBO With Cyber Liability)*

*"The [agents] **shop, research, and get us the best deals.** I look at the cost. If it's the same, if it went up a little bit, I might have a question." (SBO With Cyber Liability)*

Small businesses do not prioritize cyber insurance knowledge.

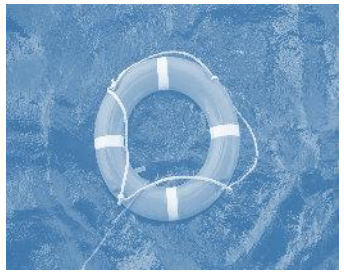
Running a small business is time-consuming.

- There is not enough time to dedicate to insurance in general, let alone to cyber.
- Small business executives are generally unable to recall details of their cyber liability policy, and trust that their agent and carrier have the necessary coverages in place.

*"I don't **even know what the coverage is**. $10,000? That feels like that's not enough." (SBO With Cyber Liability)*

*"There's **a million dollars of coverage.** I specifies different types of breaches and things. There are **different deductibles for different situations**. I could not tell you what they are." (SBO With Cyber Liability)*

However, some do want to learn more about cyber, or feel they *should* spend the time to understand it.

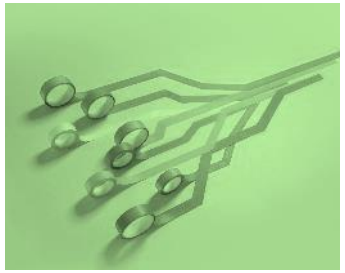


Coverage

- What does cyber cover?
- Is downtime included, or only financial losses from theft/ransomware?
- Who is covered: my company, third parties, vendors, clients?
- What are the limits? Do I have enough?

Claims support

- How long will it take to settle a claim?
- Can I stay open if I have a cyber loss?
- What are the future implications of a claim?
- Can the insurance company handle a mass event such as the CrowdStrike outage? Can it pay all those claims?



Evaluation

- Are there ways I can be a better risk, and reduce my cost?
- Should I be reviewing and updating my coverage?
- How can I re-evaluate my risk as my business changes?

Questions about cyber liability insurance…

"I might ask the insurance broker about this. It's like if we have a CrowdStrike that went down and took down half the internet with it or something like that. What happens if there's like this mass breach? Can the company cover all of the claims that might come? Sort of like hurricane insurance." (SBO with Cyber Liability)

"I would probably benefit from a session of how this coverage could help me, because there are gaps in my knowledge." (SBO With Cyber Liability)

"If a cyberattack took down my website, I don't know if that's included." (SBO with Cyber Liability)

"We probably really should revisit it. I'm assuming it's changed since we first signed up. Tailor it, with phishing and spamming, if we get more coverage there, that makes more sense versus someone trying to break into our systems." (SBO with Cyber Liability)

Implications

How can insurance carriers better support SBOs and position cyber?

To connect with SBOs on cyber liability insurance, carriers should address…

Affordability

- Offer different packages to meet budgets
- Communicate value with examples
- Discounts, bundling costs

Support

- Training opportunities/webinars
- Free risk assessment/analysis (email, app)
- Annual check ins to stay up to date

Ease

- Write all lines when possible, or package coverage ("one-stop shop")
- Online quotes for quick comparison
- Point of contact for questions

Education

- Comprehensive, concise coverage summary
- Laypersons' terms and/or definitions
- Designed for small business and/or their industry (especially industries who do not think they are at serious risk)

*"**Training would be great**, through The Hartford or the association, for free to my employees. If there were an **education session about insurance generally, cyber insurance, cybercrime,** that's something I would find value from." (SBO with Cyber Liability)*

*"Make it **easy to understand the importance.** Make it easy to understand **how you could be affected** and **why the insurance is beneficial**." (SBO With Cyber Liability)*

In summary…

- **SBOs are caught in a "push-pull" with cyber:** They know they should spend more time on cyber security issues, but they don't want to. They think they are doing the best they can.

- **They would prefer to hand this off** to someone else: their IT team, MSP, their agent/broker, their insurance carrier. They need resources they can trust.

- **Ease is the key need from insurance carriers**: Be proactive, provide information for SBOs to feel *empowered without overwhelming or shaming them*

- **Give SBOs peace of mind** with tailored coverage to their size and industry, simple tips for staying on top of emerging cyber threats, and ways to reduce cost

Thank you!

Any questions?

Kristina Witzling, EVP, P&C Practice Lead
kristina@Zeldisresearch.com

Amy Rey, Managing Director
amy@zeldisresearch.com