

modern business **IT.advisor**

"Insider Tips To Make Your Small Business Run Faster, Easier, And More Profitably"

Bay Area's Award-winning IT & Cybersecurity



TruAdvantage Recognized for Excellence
in Managed IT Services



4

THINGS TO DO NOW TO PREVENT YOUR CYBER INSURANCE CLAIM FROM BEING DENIED

October 2023



Kayvan Yazdi,
*President of
TruAdvantage*

Our Mission:

To become a trusted advisor and strategic partner to the Bay Area's SMBs and help them solve their daily issues, optimize efficiency and security and grow a competitive advantage with IT.

"Thank goodness" is probably what Illinois-based manufacturing company ICS thought about having a cyber insurance policy with Travelers Insurance after a data breach in 2022. But after claims investigators pulled out their microscopes, they found that ICS failed to use multifactor authentication (MFA) across all digital assets, which they had agreed to do in their policy. Travelers sued ICS and won. The policy was rescinded, and so were ICS's feelings of gratitude, which likely evolved into worried whispers of "Oh, crap."

Smart businesses like yours are adding cyber insurance to their policies because they know good security hygiene is just as much a competitive advantage as it is a way to reduce business risk. But with cyber insurance premiums steadily increasing – they rose 62%

last year alone – you want to make sure your claim is paid when you need it most.

Why Claims Get Denied

"Most claims that get denied are self-inflicted wounds," says Rusty Goodwin, the Organizational Efficiency Consultant at Mid-State Group, an independent insurance agency in Virginia.

Though we like to paint insurance companies as malicious money-grubbers hovering oversize "DENIED" stamps over claims, denials are usually the result of an accidental but fatal misrepresentation or omission by businesses or simply not letting an insurer know about changes in their security practices. However, there are simple steps you can take to prevent a claim-denial doomsday.

Continued on Page 2 ...

... continued from Cover

4 Ways To Make Sure Your Claim Doesn't Get Denied

1. Find a broker to help you understand your policy.

There's no doubt that insurance policies are tedious, filled with legal lingo that makes even the Aflac Duck sweat. Nevertheless, there are several parts to an insurance contract you must understand, including the deck pages (the first pages that talk about your deductible, total costs and the limits of liability), the insuring agreements (a list of all the promises the insurance company is making to *you*) and the conditions (what *you* are promising to do).

"If your broker can help you understand them and you can govern yourself according to the conditions of that contract, you will never have a problem having a claim paid," says Goodwin.

Some brokers don't specialize in cyber insurance but will take your money anyway. Be wary of those, Goodwin warns. "If an agent doesn't want to talk about cyber liability, then they either don't know anything about it or they don't care because they won't make a lot of money off it." If that's the case, he says, "take all your business elsewhere."

2. Understand the conditions.

Insurance companies are happy to write a check if you're breached *if* and only if you

make certain promises. These promises are called the conditions of the contract. Today, insurance companies expect you to promise things like using MFA and password managers, making regular data backups and hosting phishing simulation and cyber security awareness training with your employees.

Understanding the conditions is critical, but this is where most companies go wrong and wind up with a denied claim.

3. Make good on the promises.

If you've ever filled out a homeowners' insurance application, you know you'll get a nifty discount on your premium if you have a security alarm. If you don't have one, you might tick "Yes," with good intentions to call ADT or Telus to schedule an installation. You enjoy your cheaper premium but are busy and forget to install the alarm (nobody comes around to check anyway).

Then, your home gets broken into. "Guess whose insurance claim is not going to be paid?" Goodwin says. "The power is in our hands to ensure our claim gets paid. There's really nothing to be afraid of as

"Smart businesses like yours are adding cyber insurance to their policies because they know good security hygiene is just as much a competitive advantage as it is a way to reduce business risk."

long as you understand the promises that you're making."

This happens all the time in cyber insurance. Businesses promise to use MFA or host training but don't enforce it. As in the case of ICS, this is how claims get denied.

4. Don't assume that the right hand knows what the left hand is doing.

Goodwin sees companies make one big mistake with their insurance policies: making assumptions. "I see CFOs, CEOs or business owners assume their MSP is keeping all these promises they've just made, even though they never told their MSP about the policy," he says. MSPs are good at what they do, "but they aren't mind readers," Goodwin points out.

Regularly review your policy and have an open and transparent line of communication with your IT department or MSP so they can help you keep those promises.

"We're the architect of our own problems," Goodwin says. And the agents of our own salvation, if we're prepared to work with a quality broker and make good on our promises.

Free Report Download: The Business Owner's Guide To IT Support Services And Fees

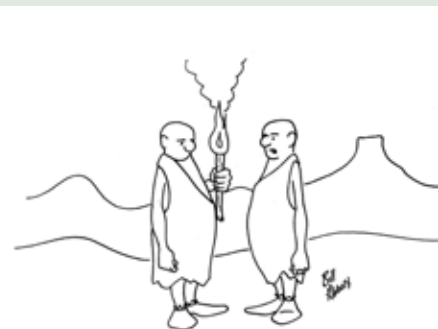
You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.TruAdvantage.com/itbuyersguide



Cartoon Of The Month



"Congratulations on the discovery.
Good luck getting it insured."

SHINY NEW GADGET OF THE MONTH**The Ooni Volt 12 Electric Pizza Oven**

Pizza is one of the most common meals eaten by Americans. The average American eats 23 pounds of pizza annually, and every day, 13% of Americans eat pizza as a meal. If you enjoy making your own fresh pizza, consider

getting an Ooni Volt 12 Electric Pizza Oven.

Unlike most pizza ovens currently on the market, you can use the Ooni Volt 12 indoors and outdoors. Its compact size makes it easy to move, and since it's electric, there's rarely a mess to clean up. The Ooni Volt 12 heats up to 850° F within 20 minutes. Once the oven has preheated, your pizza will be ready to eat in only 90 seconds. If you want to improve pizza night at your house, look no further than the Ooni Volt 12.

**Discover The Secret To Overcoming Difficult Tasks**

Throughout our lives, we all encounter obstacles that appear too daunting to overcome. During these situations, most turn to the Internet or business books for advice, but there's another source everyone should turn to for support and help: someone you trust. When you partner up with someone, regardless of whether you're starting a business, tackling a project or working toward a goal, it can make the experience less stressful. Working alongside someone allows you to brainstorm ideas and find solutions you may not have been able to come up with on your own. As the saying goes, "Two heads are better than one," so find someone to help you reach your goals and start working together.



Create The Perfect Balance

Incorporating AI While Maintaining Human Connection

ChatGPT has been a hot topic in our office lately. As an author, I immediately scoffed at it. Since ChatGPT lacks emotion, it's pretty unsatisfying. Technology constantly evolves, and we must grow with it. The question is this: How do you incorporate automation and AI into your business while maintaining integral human communication?

Automating your business and utilizing AI while maintaining your integrity and humanity can be achieved through a combination of strategies. Here are five ways to accomplish it.

Identify Areas For Automation.

Analyze your business processes and identify tasks that your team can automate without sacrificing the human touch. Look for repetitive, time-consuming activities you can streamline using technology.

Create System Recordings

And Documents. AI can't do it all! You still need humans to help run your business. But what if someone is out, has an emergency or just wants to take a sabbatical? Here's what we do in my business: For every process, our team creates a Loom recording and a Tango document to illustrate and train other team members. This means when anyone takes a four-week vacation, nothing falls to the wayside, and there are limited disruptions in productivity (read, profitability!).

Implement AI-Powered Solutions.

Leverage AI technology to automate special aspects of your business. For example, you can use chatbots or virtual assistants to handle customer inquiries, enabling human resources to respond to more complex interactions. AI can also assist in data analysis, forecasting and decision-making processes, allowing you to make informed business decisions effectively.

**Personalize Customer Interactions.**

While automation is helpful, it's essential to maintain a personalized customer experience. Tailor your automated systems to gather relevant customer information and deliver customized recommendations or responses. This can include using AI algorithms to analyze customer behavior and preferences to provide intel on marketing campaigns.

Empower Employees. Rather than replacing humans, AI can augment their capabilities and enable them to focus on meaningful tasks. Provide training for your employees so they can work alongside AI technology effectively. This might involve developing skills in areas where humans excel, such as creativity, problem-solving and emotional intelligence. Encourage collaboration between humans and AI systems to achieve optimal results.

Remember, when it comes to automation and using AI, it's crucial to balance automation and humanity! By leveraging AI and personalization, your business will be able to scale and still connect with customers and clients on a human level.



Mike Michalowicz has always believed he had the formula to success and has proven it on multiple occasions. He is the creator of the Profit First method, which hundreds of thousands of companies across the globe use to drive profit. He is the author of multiple books, including Get Different and The Toilet Paper Entrepreneur. Mike is a former small-business columnist for the Wall Street Journal and currently leads two new multimillion-dollar ventures as he puts his latest research to the test.

Inside This Issue

4 Things To Do Now To Prevent
Your Cyber Insurance Claim From
Being Denied | 1

The Business Owner's Guide To IT
Support Services And Fees | 2

How To Implement Automation While
Staying Human | 3

The Data Breach Epidemic

How Cybercriminals Are Exploiting Human Weaknesses

Every year, thousands of businesses fall victim to data breaches. In 2022, over 1,800 data compromises affected more than 422 million people, according to the Identity Theft Resource Center's 2022 Data Breach Report. As cybercriminals continue to refine their tactics, it's clear that cyber-attacks and data breaches will not stop anytime soon. That's why it's so crucial for businesses to develop strong cyber security strategies.

If you want to bolster your cyber security efforts, a great place to start is with your employees. Research from Stanford University suggests that human error is responsible for 88% of all data breaches. Here are the two common reasons why employees put their workplaces at risk of cyber-attacks.



Ignorance: Do you give cyber security training to new hires during onboarding? Do you host annual cyber security training to give your employees a refresher on what they need to know? If not, your employees might be completely unaware of what cyber-attacks can look like and how to protect the company.

Stress: If your employees are stressed out, overwhelmed and overworked, they may overlook potential cyber security concerns. Evaluate your employees' workloads and, if necessary, make adjustments to ensure nobody becomes overwhelmed.

DON'T MAKE THESE MISTAKES WHEN HIRING ONLINE

Many businesses have turned to the Internet for all of their hiring needs. They'll post open positions on job-board websites like Indeed or ZipRecruiter, create

questionnaires to prescreen potential candidates and use artificial intelligence to remove candidates with subpar résumés. Here are three online hiring mistakes you should avoid.

Not Being Descriptive Enough With Job Postings: Your candidates won't be able to clarify any questions they may have about the position before applying, so your posting needs to be as detailed as possible.

Relying Entirely On Automation: Automated screening processes can be a great tool during hiring, but you still need a human to ensure everything works as intended.

Failing To Inspect Résumés And Applications. Too many hiring managers avoid looking at résumés and applications until they interview candidates. Carefully review every application to craft relevant interview questions and find the best fit.