Connectability Corner
PUTTING THE PIECES TOGETHER.
Powered by: Connectability

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

The Secret To Hiring The Right Employees For Your Business

Hiring can be one of the most stressful situations a business leader can experience. Who you hire plays a role in every aspect of your business's success, from customer satisfaction to profitability. This leaves many wondering how to ensure they hire the right people.

Begin by carefully analyzing the potential hire's resumé and cover letter. Ensure their skills and experience are a good fit for the position while checking for grammar and spelling errors. When you bring them in for the interview, ask questions about how they handled difficult situations in the past and don't be afraid to role-play. From there, you should have them take a skills test or participate in an exercise, if applicable, to ensure they can do the job well. If everything goes well, and you think they're a good fit for the position, call their references and run a background check. Performing these steps will help ensure you hire the right person for your open position.

This monthly publication is provided courtesy of Ted Shafran, President of Connectability.

Connectability
Putting the pieces together

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

"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 multi-factor 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 The policy was rescinded, and so were ICS's feelings of gratitude, which likely evolved into worried whispers of "Oh, crap."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 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 Organized 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.

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,

continued on page 2...

...continued from cover

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.

> **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 a way to reduce business risk.**

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 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 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.

Stay Safe From Phishing Scams

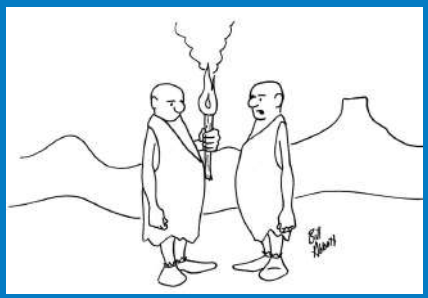
Phishing is one of the most common cyber attacks impacting businesses. In a phishing email, the hacker will pretend to be a trusted person, like a bank representative or fellow employee, to trick the receiver into sending sensitive information.

Recognize the signs of a phishing email
Phishing emails are relatively easy to detect since most of them contain the same elements. Look out for any of the following items that are common in phishing emails:

- Unusual greetings
- Messages demanding urgent action
- Content featuring many typos and grammatical errors
- Strange senders asking you for login credentials or payment information
- Unknown attachments that use files like .zip, .scr, or .exe

If you receive an email that raises your suspicion, don't click on any links or open any attachments, as they may contain malware. Report the email to us and we can mitigate the threat of further cyber attacks.

CARTOON OF THE MONTH



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

TECH CONNECT VIDEO SERIES:

The Rise of Data Breaches

If your data is breached, do you know what the costs to your business would entail? Do you know how long it could take to recover or restore your data? What are your disclosure requirements? Do you have copies of that data, or is it gone forever? What would be the impact on your clients, and would they continue to use your services after a breach?

These are all questions you should be asking yourself, and items we'll be addressing in this video.

In this video, you will learn:

- How data breaches are changing
- The Impact of a Breach (downtime, reputation damage, legal fees, etc.)
- The future of data breaches
- How data breaches can disguise other types of attacks
- How you can protect your business and clients

To watch, go to: **https://shorturl.at/mqFKW**

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.

MONTHLY CHARITY DONATION

This month we will be donating to Pathways To Education.

Pathways to Education

Pathways To Education was founded in 2001, and its mission is to help youth from low-income communities thrive. They deliver resources and support to help young people graduate from high school, and prepare for a successful future.

Using a breakthrough approach, focused on innovation and community building, Pathways To Education helps students overcome adversity by developing resiliency and skills to succeed. They focus on four important areas - academic, financial, social, and one-on-one services. Pathways To Education has helped students from all over the country graduate from high school, and has put them on the path to one day becoming Canada's leaders.

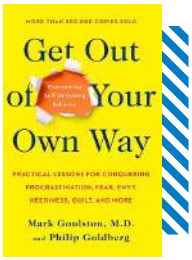
If you would like to contribute to Pathways To Education we would love your help! Email us at: info@connectability.com or call: (416) 966-3306.

Connectability
Putting the pieces together

INSIDE THIS ISSUE

GET OUT OF YOUR OWN WAY

By Mark Goulston And Philip Goldberg



As a business leader, you confront external obstacles daily. You likely have no problem devising solutions to these problems, but it becomes a different story when the challenges come from within. Most business owners' #1 enemy is themselves. They second-guess their actions, grow envious of others' successes and bottleneck important tasks while trying to devise the perfect solution. By reading *Get Out Of Your Own Way* by Mark Goulston and Philip Goldberg, you'll learn how to overcome your self-defeating behaviors. We all have self-destructive habits that prevent us from reaching our goals, even if we haven't identified them. This book offers examples and advice to identify and overcome any internal behaviors that are setting you and your business back.

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.

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.