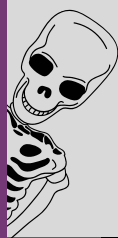


VOLUME 3
OCTOBER 2023



NEWSLETTER

WHAT'S NEW



Say hello to Dark Web Scans! This new offering will be utilized for our clients during their quarterly reviews. They will also be available to the community upon request!



As we round out 2023, our team will embark on learning the skills of a successful team, centered around "The Five Dysfunctions of a Team"



Happy 'Workiversary' to Stephen, our Technical Operations Center Team Lead!



This monthly publication is provided courtesy of Kari Renn, President of Loyalty.

Our Mission: To make IT work at work so our clients can focus on their company goals without interruption.

In This Article:

Get ready for a spooktacular October with our special cybersecurity-themed newsletter! In honor of Cybersecurity Awareness Month, we're diving deep into the dark and mysterious world of digital security. Discover bone-chilling tales of real-life cyberattacks, uncover tricks and treats to keep your online presence safe, and learn how to ward off the digital ghouls lurking in the shadows. Stay tuned for a frightfully good read!

But here's the kicker: 61% of small to midsize businesses suffer losses exceeding \$100,000 in each password-related cyberattack. And if that's not eyebrow-raising enough, picture this—51% of employees still resort to writing their passwords on sticky notes. It's like leaving the front door of your digital fortress wide open for cyber criminals.

So, what's the solution to this password peril? Enter Keeper—your knight in shining digital armor. It's the perfect addition to your cybersecurity arsenal, and here's why.



Strengthen Your Cyber Defenses: Meet Keeper - Your Ultimate Password Manager

In the world of cybersecurity, there's a chilling statistic that should send shivers down your spine: a whopping 81% of successful data breaches are a result of compromised passwords. Now, let that sink in for a moment. In an era where digital threats loom large, your first line of defense against cyberattacks could be as simple as a secure password.

Continued on pg. 2



HAPPY HALLOWEEN!

Get More Free Tips, Tools, and Services



www.loyalty.com




920-489-3187





Introducing Keeper Enterprise:


Keeper Enterprise is your fully managed, cloud-based, zero-knowledge platform designed to safeguard your most critical assets. It's not just about passwords; it's about securing infrastructure secrets like API keys, database passwords, access keys, certificates, and any confidential data you can think of.

Here's a snapshot of what Keeper Enterprise brings to the table:

 **Credential Management:** Your credentials are safely stored in the vault, out of reach from prying eyes – no more need for sticky notes.

 **Integration Power:** Seamlessly integrated with top CI/CD systems to streamline your workflow.

 **Centralized Control:** Centralized management and Role-Based Access Controls (RBAC) for fine-grained access control.

 **Visibility and Compliance:** Robust reporting, alerts, audits, logs, and SIEM integration to maintain compliance standards.



81% of successful data breaches are a result of compromised passwords




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 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 over "DENIED" stamps over claims, denials are usually the result of an accidental but fatal misrepresentation or omission by businesses or simply not

 **Privileged Access Management:** Lightning-fast, agentless, web browser access with zero-trust security and session recording.

 **Single Sign-On (SSO) Integration:** Easily deploy Keeper with existing SAML 2.0-compatible SSO solutions.

 **Scalable User Provisioning:** Streamline onboarding through advanced integration with AD, SSO, SCIM, and APIs.

 **Team Collaboration:** Securely create, share, and manage records and encrypted folders across teams.

 **Advanced DevOps Tools:** The Keeper Commander SDK offers open-source code, command-line tools, and APIs for password management.



And the best part? Keeper is SOC 2 Certified, ISO27001 Certified, FedRAMP Authorized, and StateRAMP Authorized. Its encryption is NIST CMVP certified and validated to the FIPS 140 standard by accredited third-party laboratories. With millions of users worldwide, Keeper is the proven industry leader in cybersecurity.

So, here's your October challenge: In Cybersecurity Awareness Month, take the step to fortify your defenses. Reach out to your vCIO to learn more about Keeper and how it can be your trusty sidekick in the battle against cyber threats. Your digital castle deserves the best protection, and Keeper is here to deliver it. Don't let those passwords haunt you any longer—take control with Keeper today!

letting an insurer know about changes in their security practices. However, there are simple steps you can take to prevent a claim-denial doomsday.

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."

Continued on pg. 3





2. Understand the conditions.

Insurance companies are happy to write a check to cover a breach 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.

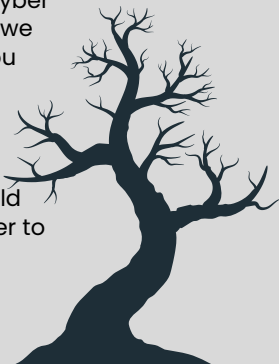
3. Make good on the promises.

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 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. We can also be the agents of our own salvation, if we're prepared to work with a quality broker and make good on our promises.

In essence, the power to ensure your claim gets paid lies in your hands. By collaborating with a knowledgeable broker, comprehending your policy conditions, fulfilling your commitments, and maintaining effective communication within your organization, you can significantly reduce the risk of a denied cyber insurance claim. At Loyalty, we are committed to helping you navigate the technology implications and standards involved in maintaining your policy to protect your business effectively. We would happily meet with your broker to ensure your cybersecurity practices align with your policy, securing your organization's digital future.



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 three ways to accomplish it.

- 1 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.
- 2 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.
- 3 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.

Recommend Loyalty and get a \$200 VISA for every qualified appointment booked.

Loyalty will meet with your referral and determine if we are a good fit for their IT needs.

Loyalty will propose a best-fit solution to solve their IT problems and concerns.

Loyalty it's our word.
REFERRAL PROGRAM

Your referral becomes a Loyalty client - you get a \$1,000 VISA!!

Get More Free Tips, Tools, and Services



www.loyalty.com



920-489-3187



The Data Breach Epidemic: How Cybercriminals Are Exploiting Human Weaknesses



Every year, thousands of businesses all over the country 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. Neglecting cyber security training, both during onboarding and through annual refreshers, can lead to employee ignorance about cyber-attacks and how to safeguard the company, leaving your organization vulnerable to potential threats.

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.

Hiring Mistakes: What To Avoid 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.



The power of layered defense was showcased once again when one of our clients faced a potential security threat.

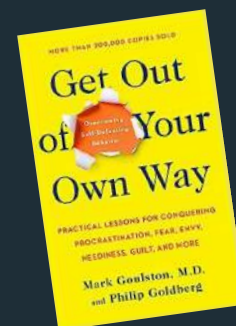
Thanks to the swift detection and response from Barracuda and our dedicated team, the situation was remedied. This incident serves as a reminder that, regardless of the technical tools in place, users can be the weakest link. By closely monitoring audit logs, we identified suspicious login attempts from other countries. We discovered that the user had fallen victim to a phishing email, highlighting the importance of user education and vigilance. This successful response underscores the effectiveness of a robust cybersecurity strategy.



READING CORNER

Get Out Of Your Own Way

By Mark Goulston And Philip Goldberg



As a business leader, you often face external obstacles, but the most significant challenges often stem from within. In 'Get Out Of Your Own Way' by Mark Goulston and Philip Goldberg, you'll discover how to overcome self-defeating behaviors that hinder your success. This book provides examples and guidance to help you identify and conquer internal barriers holding you and your business back.



Are YOUR Credentials On The Dark Web? With Our Free Scan, You'll Know:



- ✦ What credentials (if any) are actively being SOLD on the Dark Web
- ✦ If your company (and your reputation) are at risk
- ✦ If your customers' private information is at risk

Claim your FREE no obligation Dark Web Scan at
www.loyalty.com/dark-web-scan/

Get More Free Tips, Tools, and Services



www.loyalty.com



920-489-3187