March 2024

TechTidbit.com

brought to you by Tech Experts

How Can A Data Breach Cost Your Company For Years?

Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

The repercussions of a data breach extend far beyond the immediate aftermath. They often haunt businesses for years.

Only 51% of data breach costs occur within the first year of an incident. The other 49% happen in year two and beyond.

Only 51% of data breach costs occur within the first year of an incident. The other 49% happen in year two and beyond.

The unseen costs of a data breach

The First American Title Insurance Co. case is a good example.

The 2019 cybersecurity breach at First American serves as a stark illustration. It reminds us of the far-reaching consequences of a data breach. In this case, the New York Department of Financial Services (NYDFS) imposed a $1 million fine.

Cybersecurity sites announced the fine in the fall of 2023. The company's fine was for failing to safeguard sensitive consumer information. This is one example of how costs can come long after an initial breach.

Lingering impacts of a data breach

The financial toll of a data breach is significant. Immediate costs include things like breach detection, containment and customer notification.

Beyond those, businesses face long-term expenses. These relate to legal battles, regulatory fines, and reparations.

Reputational damage

The impact on a business's reputation is arguably the most enduring consequence. Customers lose trust in a company's ability to protect their sensitive information. This loss of trust can result in a decline in customer retention. As well as acquisition difficulties and long-lasting damage to the brand image.

Regulatory scrutiny

Regulatory bodies increasingly hold businesses accountable for safeguarding consumer data. A data breach triggers regulatory scrutiny. This may lead to fines and ongoing compliance requirements.

Operational disruption

The aftermath of a data breach disrupts normal business operations. Companies must take remediation efforts and put in place enhanced security measures. These can divert resources away from core business functions.

Customer churn and acquisition challenges

A data breach often leads to customer churn. Individuals lose confidence in the business's ability to protect their data.

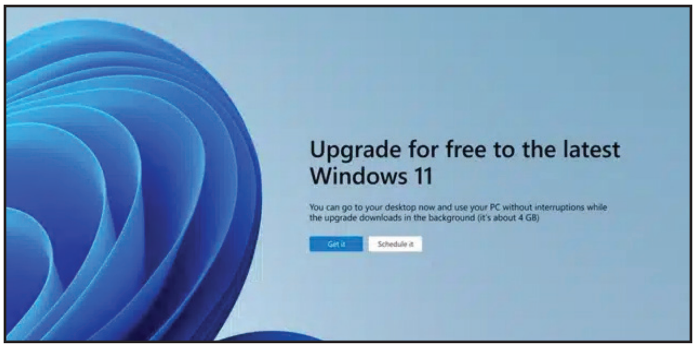
Acquiring new customers becomes challenging. Potential clients are wary of associating with a brand that has suffered a breach. The prolonged effects on customer acquisition can hinder the company's growth as well as its market competitiveness.

A cautionary tale for businesses everywhere

The repercussions of a data breach extend far beyond the immediate incident. They can impact the financial health and reputation of a business for years as well as its regulatory standing.

Are You Really Ready To Upgrade To Windows 11?

> *"Before you get all excited about Windows 11, check which of your current PCs can handle the upgrade. Some older machines might not meet the system requirements, and you don't want any surprises down the road."*



Upgrade for free to the latest Windows 11

You can go to your desktop now and use your PC without interruptions while the upgrade downloads in the background (it's about 4 GB)

So, you're thinking about upgrading your business to Windows 11? That's a smart move because this update comes with some cool features that can boost your productivity.

But here's the thing, it's not as simple as clicking a button and SHAZAM, you're on Windows 11. You need a plan, or you might end up with some messy downtime and confused employees.

Before you get all excited about Windows 11, check which of your current PCs can handle the upgrade. Some older machines might not meet the system requirements, and you don't want any surprises down the road.

If you need to replace some computers, make sure you budget for that as part of your upgrade plan.

Most of your software that works on Windows 10 should play nice with Windows 11, but don't take that for granted.

Look at all the software your business relies on to make sure it won't freak out with the new operating system (OS). Some software might need updates to get along with Windows 11, so keep an eye on that too.

Whenever you're making a big change that affects your team, you've got to have a plan. It's your roadmap to success. So, what should your upgrade plan include?

- Clear and honest communication with your team about the upgrade
- Training sessions to show your employees the ropes of the new OS
- Help for your managers to guide their teams
- A timeline for when the upgrade will happen, and all the communication and training that goes with it
- A plan to handle any bumps in the road and any resistance you might encounter
- A resource to help your team with any questions or issues they have after the upgrade

Alternatively, team up with an IT support partner (like Tech Experts) to make sure everything goes smoothly and to take the weight off your shoulders!

Don't go solo on this one; it's best to have IT pros in your corner. If something goes wrong during the upgrade and you've done it yourself, it might take a lot longer to get things back on track. Let experts like our team handle it. We know what we're doing.

Upgrading to Windows 11 can supercharge your business, but only if you plan.

If you'd like help to make the change as smooth as can be, get in touch.

We Love Referrals!

The greatest gift anyone can give us is a referral to your friends and business colleagues. Referrals help us keep costs down so we can pass the savings to our clients.

If your friend ends up becoming a client - we'll give them their free first month of service (for being a friend of yours) AND we'll give you a $250 Amazon Gift Card.

Simply introduce us via email to sales@mytechexperts.com and we'll take it from there. We'll look after your friend's business with a high level of care and attention (just like we do with all our clients).

Unlocking Business Potential With Generative AI: A Guide For Non-Technical Business Owners

In an age where technology continually reshapes the landscape of how we do business, staying informed and adaptable is key. As a non-technical business owner, you might have heard about the buzz surrounding generative AI, but what exactly is it, and more importantly, how can it benefit your small business? This article breaks down the essentials of generative AI and provides practical ways to integrate this innovative technology into your business strategy.

Understanding generative AI

Generative AI refers to artificial intelligence that can generate new content, from written text to images, and even music. This technology, powered by sophisticated algorithms, learns from existing data to create original, realistic outputs. The most common examples you might have come across include chatbots, image generators, and content creation tools.

Enhance customer service with AI chatbots

One of the most immediate applications of generative AI for small businesses is through AI chatbots. These virtual assistants can handle customer inquiries, provide product recommendations, and offer support 24/7. This not only improves customer satisfaction but also frees up your staff to focus on more complex tasks. Tools like OpenAI's GPT-3 have made creating these chatbots more accessible than ever.

AI-generated content boosts online presence

Creating engaging content consistently can be a daunting task for many business owners. Generative AI comes to the rescue by assisting in generating blog posts, social media updates, and even marketing copy. Tools like Jasper or Writesonic can help you craft compelling content that resonates with your audience, saving you time and resources.

Personalizing customer experiences

Personalization is a key differentiator in today's market. Generative AI can analyze customer data to create personalized recommendations, tailored emails, and targeted advertising campaigns. This level of personalization can significantly enhance customer engagement and loyalty.

Streamlining operations with automated processes

Generative AI can also play a pivotal role in streamlining business operations. For instance, AI can automate invoice generation, schedule appointments, and even manage inventory. This not only increases efficiency but also reduces the likelihood of human error.

Exploring creative possibilities with AI generated designs

For businesses that rely on creative outputs like graphics, marketing materials, or product designs, generative AI offers a world of possibilities. Tools like DALL-E or Canva's Magic Write can generate high-quality images and designs based on your specifications, providing a cost-effective alternative to hiring designers.

Understanding the limitations and ethical considerations

While generative AI offers numerous advantages, it's important to be aware of its limitations and ethical implications. AI-generated content may require human oversight to ensure accuracy and relevance. Additionally, issues around data privacy and intellectual property rights in AI-generated content are important to consider and navigate carefully.

Generative AI is not a distant, high-tech dream but a tangible tool that small businesses can leverage today to drive growth, enhance efficiency, and create engaging customer experiences. By understanding and integrating this technology into various aspects of your business, you can stay ahead in a competitive market.

As you explore generative AI options, remember that the key is to use these tools as a complement to human creativity and expertise, not a replacement. Embracing AI smartly can unlock new horizons for your business and pave the way for future innovations.

Start small and experiment with AI tools relevant to your business needs. Whether it's enhancing customer service, content creation, or operational efficiency, the journey into the world of generative AI promises to be both exciting and rewarding for forward-thinking business owners.

Reader's Note

The article to the left was written entirely by AI using the prompt *"write a newsletter article geared toward non technical business owners about how to use generative AI in their small businesses."*

We then asked Chat GPT to create an image to accompany the article. The image you see was also generated by AI.

This is a technology that goes beyond automation and the AI we used to know. It can create content, solutions, and possibilities before unimaginable.

The landscape of small business marketing is evolving rapidly. The integration of AI technologies is reshaping strategies for growth. Small businesses are turning to GenAI to enhance their marketing efforts.

Despite how useful AI can be, it isn't a replacement for human review, tweaking and approvals. For example, the image that ChatGPT generated contains some misspellings.

Online Security: Addressing The Dangers Of Browser Extensions

Browser extensions have become as common as mobile apps. People tend to download many and use few. There are over 176,000 browser extensions available on Google Chrome alone. These extensions offer users extra functionalities and customization options.

While browser extensions enhance the browsing experience, they also pose a danger. Which can mean significant risks to online security and privacy.

The allure and perils of browser extensions

Browser extensions are often hailed for their convenience and versatility. They are modules that users can add to their web browsers. They extend functionality and add customizable elements.

From ad blockers and password managers to productivity tools, the variety is vast. But the ease with which users can install these extensions is a weakness. Because it also introduces inherent security risks.

Key risks posed by browser extensions

Many browser extensions request broad permissions. If abused, they can compromise user privacy. Some of these include accessing browsing history and monitoring keystrokes. Certain extensions may overstep their intended functionality. This can lead to the unauthorized collection of sensitive information.

Users often grant permissions without thoroughly reviewing them. This causes them to unintentionally expose personal data to potential misuse.

There are many extensions developed with genuine intentions. But some extensions harbor malicious code. This code can exploit users for financial gain or other malicious purposes. These rogue extensions may inject unwanted ads. As well as track user activities or even deliver malware.

These extensions often use deceptive practices. They make it challenging for users to distinguish between legitimate and malicious software.

Extensions that are no longer maintained or updated pose a significant security risk. Outdated extensions may have unresolved vulnerabilities. Hackers can exploit them to gain access to a user's browser. As well as potentially compromising their entire system. Without regular updates and security patches, these extensions become a liability.

Some malicious extensions engage in phishing attacks. As well as social engineering tactics. These attacks can trick users into divulging sensitive information.

This can include creating fake login pages or mimicking popular websites. These tactics lead unsuspecting users to unknowingly provide data. Sensitive data, like usernames, passwords, or other confidential details.

Best practices for browser extension security

Download extensions only from official browser marketplaces. Such as those connected with the browser developer (Google, Microsoft, etc.). These platforms have stringent security measures in place. This reduces the likelihood of encountering malicious software.

Before installing any extension, carefully review the permissions it requests. Be cautious if an extension seeks access to unusual data. Such as data that seems unrelated to its core functionality. Limit permissions to only what is essential for the extension's intended purpose.

Regularly update your browser extensions. This ensures you have the latest security patches. Developers release updates to address vulnerabilities and enhance security. If an extension is no longer receiving updates, consider finding an alternative.

It's tempting to install several extensions for various functionalities. But each added extension increases the potential attack surface. Only install extensions that are genuinely needed. Regularly review and uninstall those that are no longer in use.

Use reputable antivirus and antimalware software. This adds an extra layer of protection against malicious extensions. These tools can detect and remove threats that may bypass browser security.

Stay informed about the potential risks associated with browser extensions. Understand the permissions you grant. Be aware of the types of threats that can arise from malicious software. Education is a powerful tool in mitigating security risks.

Don't stay in the dark about your defenses. We can assess your cybersecurity measures and provide proactive steps for better protection. Give us a call today to schedule a chat.

Contact Information

Tech Experts
Support Team
(734) 240-0200
support@MyTechExperts.com

Main Office
(734) 457-5000
info@MyTechExperts.com

Sales Inquiries
(888) 457-5001
sales@MyTechExperts.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com

Tech Experts® and the Tech Experts logo are registered trademarks of Tech Support Inc.