1991 – 2021
30 YEARS OF EXCELLENCE
Computer Technologies, Inc.

TECHNOLOGY TIMES

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

What's Inside

May 2022

Kim Nielsen
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

How to Protect Your Fast-Growing Business From a Data Breach

In this article, we expose how vulnerable most businesses are to cyberattacks and what company management can do about it. Consider this; in the first half of 2019, data breaches exposed 4.1 billion records, and yet many companies still mistakenly believe they're impervious to a data breach.

This mindset is problematic as cybercriminals are becoming significantly more sophisticated, targeting all sized businesses with multi-tiered attacks. The threat of experiencing a data breach is massive. It's a setback that could stall your fast-growing company for months. What's worse, a data breach could bottleneck your progress indefinitely or cause you to shutter. Here's how to protect your company from a harmful data breach.

What's a Data Breach?

According to the US Department of Justice, a breach is:

"The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information (PII) or (2) an authorized user accesses or potentially accesses PII for other un authorized purpose. It includes both intrusions (from outside the organization) and misuse (from within the organization)."

In short, a data breach occurs when a cybercriminal gains unauthorized access to private or personal files. In the past decade, cybercriminals have compromised over 100,000 digital files. Some of the most at-risk industries include Healthcare, SaaS, and critical infrastructure, to name a few. Truthfully, any company is a potential target.

Top 3 Data Breach Protections

Here are a few practical ways a rapidly-

Continued on pg.2

Continued from pg.1

evolving business can protect itself against these disruptive crimes.

1. Establish Identity Management

Ideas and practices flow from the head down, which means that cybersecurity starts with management. To begin with, company leaders must establish and enforce reliable identity management processes. This cautious approach means:

- Monitoring privileged account security policies
- Maintaining adequate IT support
- Keeping a password policy
- Require security awareness training

As mentioned, it's not uncommon for company leaders to belong to an "it won't happen to us" school of thought. Unfortunately, many victims of cyberattacks believed the same thing and became lax with their identity management.

2. Support Security Awareness

The four main strategies cybercriminals use to steal information include:

- **Malware** – malicious software that harmfully probes systems
- **Ransomware** – software that gains access to and then restricts access to vital information
- **Phishing** – scams where hackers gain access to confidential information from an email that was received.

Business must be vigilant to battle the secretive master plans of cybercriminals. No longer can leaders depend solely on their IT staff to protect vital data. Instead, companies must train employees to spot cyber threats and handle the company's data correctly, including:

- No hard-coding or embedding passwords
- Deactivating unused credentials
- Managing identity controls

Additionally, fast-growing businesses can't slack on software updates. These updates are essential to ongoing security of your data and IT assets. Although increased security awareness takes more time and diligence, the results are well worth it.

3. Practice Resiliency

Some cyberattacks, such as phishing and malware, steal vital data with the intent of profiting from its use. Other attacks, such as ransomware and DoS, disrupt business operations as opposed to taking data outright.

Additionally, consider what would happen to your business if a natural disaster occurs. Suppose a fire, flood, or tornado tore through your office over the weekend. Does your company have a business continuity plan? What about a disaster recovery plan? Do you have other copies of your company's vital data so business operations can carry on?

Having professional resilience typically means being prepared for the worst-case scenario while hoping for the best. That said, resiliency is critical in terms of handling disruptive risk and can help to protect from a data breach.

To sum up, prepare for business disruptions by storing several copies of your vital data elsewhere. And have a recovery plan in place, so you aren't scrambling when the time comes.

It's not uncommon for company leaders to belong to an "it won't happen to us" school of thought.

Do You Safeguard Your Business And Your Customers' Private Information BETTER THAN Equifax and Target Did?

If the answer is "NO" – and let's be honest, the answer *is* no – you are leaving yourself and your company open to massive liability, ***millions*** in fines and lost business, lawsuits, theft and so much more.

Why? Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – social security numbers, credit card numbers, birth dates, home addresses, e-mails, etc.

Don't kid yourself. Cybercriminals and hackers will stop at NOTHING to steal your credentials. And once they have your password(s), it's only a matter of time before they destroy your business, scare away your customers and ruin your professional and personal life.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Our 100% FREE and 100% confidential, exclusive Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully it will be ALL CLEAR and you can breathe easy. If your company, your profits, and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let this happen to you, your employees and your customers. *Reserve your exclusive Dark Web Scan **now**!*

Get your free Dark Web Scan TODAY at:
https://www.cti-mi.com/dark-web-scan-522

Security Corner

Clickjacking: What Is It and How Can It Affect Your Business?

Organizations spend a lot of time and money training their employees how to recognize and react to cyber threats when they spot one in their system. While you've been preparing phishing tests to send out, though, this doesn't prepare employees for the unfortunate circumstance where someone successfully tricks them into giving out private information without them even noticing.

It can happen in a few ways, one of which is called **clickjacking**. By changing the interface of a website without any visible sign, users will input their own private credentials without knowing it's going directly into a cybercriminal's hands.

What is Clickjacking?

With clickjacking, a hidden website or login box is rendered on top of where the legitimate content typically goes. Frequent visitors of the site therefore see nothing wrong when they go to enter their information. Then hackers can: Steal login info, turn on your webcam or microphone remotely to eavesdrop, or spread worms or malware to your friend's list

Types of Clickjacking

- **Cookiejacking**: Capturing your cookies to expose saved credentials
- **Nested clickjacking –** Also known as UI redressing, this injects malicious frames between two otherwise harmless frames on the page to avoid browser detection
- **Likejacking –** Specific to Facebook, this refers to layering invisible pages over seemingly-normal Facebook pages that "Like" the page and spread spam, no matter where you click

For more information on Clickjacking and how to prevent falling victim, call us at 248-362-3800 or visit: https://bit.ly/3vxpyt0

Tools That Every Business Should Have

Technology is expanding its roots across all areas of the business world. Similarly, technology is making a massive impact on the hiring process. By integrating an AI-based recruitment tool, recruiters access candidates' profiles and get an easy platform to post and manage job applications. Modern AI technology is growing popular and making recruitment tasks effective and efficient.

You can seek help from Artificial Intelligence technology to find a perfect candidate. Numerous tools are available online for this purpose. This software is perfect for hiring managers and recruiters as it improves their processes. Developers use these AI tools for numerous algorithms, such as Google algorithms, to predict customer searches. Similarly, this artificial intelligence algorithm also helps businesses recruit qualified candidates quickly. Here are some of the ways AI helps in recruitment tasks:

Sourcing Candidates
AI reduces your time to find and recruit a potential candidate. Your recruiters no longer have to browse through LinkedIn profiles, attend career fairs, and post jobs online to find eligible candidates. With artificial intelligence, you can automate these tasks and find candidates while focusing on other tasks.

Screening Applications
Artificial intelligence can sort all the resumes from candidates so you can make a better decision based on qualification and skills. It isn't possible for humans to analyze and sort all the job applications accurately and quickly. With AI, you can screen hundreds of resumes and search for the best candidate with relevant past experience and other qualities, reducing the time it takes to review applications.

Communication
Artificial Intelligence facilitates you with better communication with the candidates. Businesses use Chatbots for customer services. Now you can use the same technology to reach qualified applicants, allowing you can gather their information and call them for an interview. These advances enable you to analyze candidates' personalities to help you choose a better candidate.

Candidate Experience
Most candidates don't receive a good response from recruitment teams. Sometimes, they fail to receive a response, once they send the resume and job application. This can create a negative candidate experience, affecting your business credibility in the market. If you want to hear from the candidate, you can provide a positive experience by automating an AI-based recruitment tool to your business.

Reduce Bias
Other than improving the candidate experience and saving your time, you can use artificial intelligence to reduce bias in the recruitment process. When you use the workforce to hire that the recruitment teams give biased responses. So with AI recruitment tools, you can diversify your teams, neglecting all racial, religious, and gender biases.

In conclusion, business owners are still unsure if they should adopt AI-powered recruitment tools for their business. They are struggling to trust artificial intelligence and consider the workforce better than these advanced technologies. However, it is essential to understand that artificial intelligence is not a competition. Rather, it is a tool to facilitate and streamline arduous tasks.

Steps to Motivate Your Employees Towards A Similar Goal

Project management tools motivate your employees to focus on similar business goals. These tools manage workflow and help with time -management. Moreover, it brings efficiency in handling problems and helps manage resources. Here are some of the steps you can take to direct your employees to a similar goal while utilizing project management tools:

- Plan and schedule the tasks and projects accordingly, bringing efficiency to the workflow
- Maintain better collaboration and reduce errors and inaccuracies in the workplace
- With this project and time management tool, allocate tasks while considering employees' capabilities and skills
- Offer employees easy and straightforward techniques to share, receive, and access files
- Integrate new employees easily with the simple interface of the tool
- Lower the risk of mitigation through proper management and accountability of all of your employees

Choosing professional and efficient software enables you to efficiently collaborate and increase projects' success rates. Numerous options are available online so pick the best one that fulfills all your needs and requirements and bring all your employees to the same platform.

The Benefits Of An Electronic Signature

Many businesses prefer handwritten signatures over electronic. Here are some benefits of a digital signature and why your business may want to adopt this technology:

- Electronic signature enables you to communicate and collaborate globally. It also facilitates your business functions with remote authentication.
- This technology ensures added security over traditional paper documents. You can easily conduct transactions with this enforceable and stronger online signature system.
- This new technology reduces your energy and time as all the documents are digital.
- It facilitates communication with the clients keeping them satisfied and happy.
- Environmentally friendly way to decrease paper production and help protect the environment.

NEED A LAUGH?

What is an astronaut's favorite place on a computer?

The space bar!