VOLUME XIV ISSUE 10
OCTOBER 2023
OTTAWA ON

TECHLORE

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

"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!"
-Ruben Diaz
NeoLore Networks

Essential Cybersecurity Practices to Protect Your Digital Assets

Research shows that 53% of organizations suffered a third-party breach last year. So, it's no surprise that companies worldwide plan to spend 11.3% more on cybersecurity.

When it comes to your company, you must take the time to understand how you can protect your digital assets against a growing army of cyber threats. Below we'll discuss what digital assets are and the top cybersecurity practices to defend them.

Digital assets refer to any online material, such as the information live on your company's server and stored in the cloud. It comprises audio files, blogs, a customer database, images, slides, social media, and videos.

Let's dive into the top five cybersecurity practices businesses must use to protect their digital assets:

Investing in Digital Asset Management

Enhance digital asset security by leveraging digital asset management (DAM) software to store sensitive data. That way, you can access your information from a safe and centralized folder without worrying about unauthorized access.

Most DAM requires individuals to showcase their permits before unlocking digital assets. As a result, you can implement permission-based access to keep your confidential data safe from prying eyes.

Encrypting Your Sensitive Files

Another fantastic way to secure your online data is by encrypting your files. It converts sensitive data into complex code to minimize the risk of unauthorized access. That way, no hacker can understand the information stored in your digital asset.

At the same time, authorized users have to use a specific binary to decode the encrypted digital files. As a result, you can bolster your business's safety by using robust encryption software.

Implementing Strong Access Controls

Although insider threats are tricky to catch, you can easily control them by implementing a top-notch control system. It helps you to limit employees' access to the customer database, confidential data, and organizational information.

Ensuring Employees are Up-to-Date

It's no secret that your employees need access to your digital assets to complete and manage their tasks effectively. Therefore, training your workers to minimize intentional human errors and strategies to avoid online attacks makes sense.

Some cybersecurity issues can be rooted in an employee's lack of knowledge about baking Trojans, malware, phishing attack, and malware. For instance, your worker might not know that sharing digital assets or sharing passwords puts your company at risk.

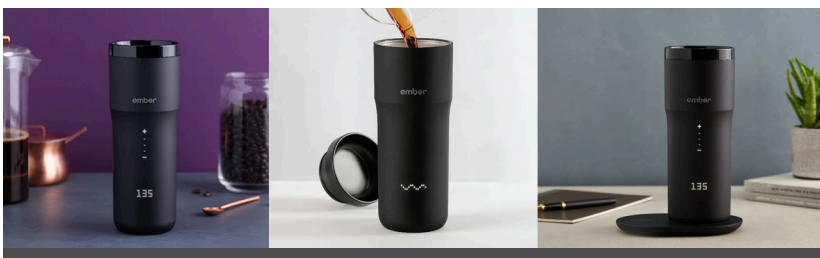
Backing Up Your Digital Asset Files

Here's the thing: hackers are constantly finding new ways to access your protected and sensitive data. So, to eradicate the risks of losing all your data, you must create and store a backup plan on an external drive, or cloud system.

Updating and Maintaining Your Systems

Technology is rapidly advancing, so hackers and cybercriminals can access the latest tech to penetrate your business networks. Therefore, businesses should stay updated with the latest software advancements to minimize security risks.

With continuous security patches and system updates, you can address vulnerabilities, minimize the risk of hackers' exploitation, and reduce cybercriminals' attacks.



Ember Travel Mug 2

Designed to be used on-the-go, the Ember Travel Mug² does more than simply keep your coffee hot. Our smart heated travel mug allows you to set an exact drinking temperature and keeps it there for up to 3 hours, so your coffee is never too hot, or too cold. Ember Travel Mug² is easy to clean and is safe to handwash and submersible up to 1 meter in water. The leak-proof lid is dishwasher safe. Get yours at ember.com

VOLUME XIV ISSUE 10
OCTOBER 2023
OTTAWA ON

Selecting the Ideal Cloud Computing Model for Business Success: SaaS vs. PaaS vs. IaaS

What are the Three Primary Cloud Computing Services?

Before determining which cloud service is perfect for your organization, let's discuss the basics. Cloud computing is the real-time delivery of various services via the Internet. Cloud computing involves three primary models: flexibility, management needs, and control. These include:

- SaaS – Software as a Service is a ready-to-go and easy-to-access software available on the Internet and delivered as a cloud service.
- PaaS – Platform as a Service is an amalgamation of SaaS and IaaS, offering a flexible and scalable platform to run and manage apps.
- IaaS – Infrastructure as a Service offers a pay-as-you-go model where the provider hosts computing, storing, and networking components.

How to Select the Best Cloud Computing Model for Your Business?

Let's now explore how you can select the ideal cloud computing model for your organization:

SaaS

Software as a Service delivers your software without having to install it on your company's computers and servers. You can access your software once you set up a stable Wi-Fi connection!

Besides this, your SaaS vendor will take the stress of handling app functioning off your shoulders.

SaaS is ideal for small businesses, startups, and freelancers with limited budgets. The cloud computing model can help users save costs while providing a simplified and intuitive interface.

PaaS

It provides users with a robust platform with built-in components and tools so companies can handle application development while vendors manage their infrastructure. With PaaS, businesses can boost and simplify software development.

PaaS is perfect for businesses collaborating on projects with multiple developers and vendors. This model can help minimize the operational burden on IT teams while bolstering efficiency.

IaaS

Infrastructure as a Service is the most straightforward cloud computing model where organizations rent various components from vendors.

Therefore the users can install, manage, maintain, and support their ap ps and software, whereas the vendor handles the infrastructure.

IaaS is ideal for small, mid, and large businesses as it offers you access to essential computing resources. Moreover, it lets you upsize your infrastructure based on business growth.

Emerging Challenges Faced by Evolutionary Computation

Evolutionary Computation (EC) is an emerging technology driven by Artificial Intelligence (AI) and inspired by natural evolution. The powerful computational intelligence strategy is vital in solving and enhancing optimization problems.

But despite its endless use and limitless potential, the technique faces significant challenges. Below we'll explore the basics of EC and its primary issues:

A Quick Glance at Evolutionary Computation

Evolutionary Computation, or EC, is a subcategory of AI for solving problems with multiple variables. The robust technique facilitates continuous system and structure optimization.

Typically, computers using EC run genetic algorithms, evolutionary programming, and swarm intelligence models like particle swarm optimization.

Emerging Challenges in the EC Field

Here are the different challenges faced by EC:

- Inability to reproduce experiments
- Issues in Bridging Theory and Practice
- Making EAs user-friendly for non-EA experts

Evolutionary computation utilizes powerful algorithms that evolve and improve with the availability of data and experience. While this technique helps businesses refine weaker solutions, it faces several foundational challenges.

As AI advances, the solutions to the challenges discussed will likely emerge.

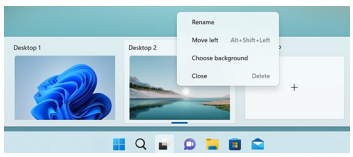
Understanding Network Architectures and Security

It's easier today than ever to log onto a website and access information. But behind this convenience is a complex mechanism of network devices and services. The magnetic structure of these wires, cables, and servers tailored to meet the connectivity needs of a business is network architecture. Network security architectures lay the foundation for a company's cyber protection, minimizing the risk of unauthorized access and protecting IT assets. Typically, a network security architecture includes the following elements:

- Network Elements include network nodes, communication protocols, connection media, and topologies.
- Security Elements involve cyber security devices, software, and data privacy tech.

Use Multiple Desktops in Windows 11

Multiple desktops is an upgraded Windows 10 feature. To use it, you need to enable the Task View icon in your taskbar (Settings -> Personalization -> Taskbar). Click it to add a new desktop. You can then easily switch between them by hovering over the icon and selecting the desktop you want to use.



New for Windows 11, you can also change the wallpaper for each desktop to make it easier to identify at a glance. Whatever theme you've selected will be applied across the board, though.

Significant Impacts of Neural Networks

Artificial Neural Network (ANN) is a fascinating breakthrough in AI based on Machine Learning. It encourages computers to mimic our brain's neural network. The structure is based on layers of interconnected nodes to create an adaptive system for computers.

Primary Types of Neural Networks

Neural networks can be of various types based on their purpose:

Convolutional Neural Networks – These involve five layers and focus on image classification.

Recurrent Neural Networks – RNNs contain sequential information and are used in forecasting applications.

Why Are NN Important?

Neural networks are vital in helping users solve complex real-life problems and improve decision-making. Here's why it's crucial:

- Diagnosing medical and disease
- Creating robotic control systems
- Evaluating ecosystems

Take the NeoLore Cyber Security Survey

Has your company done a Cyber Security Maturity Assessment within the last year? Do you have an IT security policy in place? Do you know if you've been hacked or are leaking data?

If your answer was "no" or "I'm not sure" to any of those questions, your company may be at risk for a devastating cyberattack.

Get the NeoLore Networks Cyber Security eBook for Free!

It Features

- Information on the various threats to your business
- NIST Security Framework
- CIS Controls
- Basic Controls

And More!

https://neolore.com/cybersecurity