TECHNICAL FRAMEWORK
IT FOR EVERYONE, EVERYWHERE

(970) 372-4940
info@techframework.com
https://techframework.com

How to Organize Your Cybersecurity Strategy Into Left and Right of Boom

TECH INSIDER

December 2023

Corporate

Personal & Home-Office

Websites

CORPORATE

How to Organize Your Cybersecurity Strategy Into Left

and Right of Boom

In the pulsating digital landscape, every click and keystroke echoes through cyberspace. The battle for data security rages on. Businesses stand as both guardians and targets. Unseen adversaries covet their digital assets.

Businesses must arm themselves with a sophisticated arsenal of cybersecurity strategies. On one side, the vigilant guards of prevention (Left of Boom). On the other, the resilient bulwarks of recovery (Right of Boom).

Together, these strategies form the linchpin of a comprehensive defense. They help ensure that businesses can repel attacks. And also rise stronger from the ashes if breached.

What Do "Left of Boom" and "Right of Boom" Mean?

In the realm of cybersecurity, "Left of Boom" and "Right of Boom" are strategic terms. They delineate the proactive and reactive approaches to dealing with cyber threats.

"**Left of Boom**" refers to preemptive measures and preventative strategies. These are things implemented to safeguard against potential security breaches. It encompasses actions aimed at preventing cyber incidents before they occur.

"**Right of Boom**" pertains to the post-breach recovery strategies. Companies use these after a security incident has taken place. This phase involves activities like incident response planning and data backup.

Together, these terms form a comprehensive cybersecurity strategy. They cover both prevention and recovery aspects.

Left of Boom: Prevention Strategies

User Education and Awareness

One of the foundational elements of Left of Boom is employee cybersecurity education. Regular training sessions can empower staff.

Access control tactics include:

- Least privilege access
- Multifactor authentication (MFA)
- Contextual access
- Single Sign-on (SSO) solutions

Regular Software Updates and Patch Management

Left of Boom strategies include ensuring all software is regularly updated.

Network Security and Firewalls

Firewalls act as the first line of defense against external threats. Install robust firewalls and intrusion detection/prevention systems.

Regular Security Audits and Vulnerability Assessments

Conduct regular security audits and vulnerability assessments. This helps to identify potential weaknesses in your systems.

Right of Boom: Recovery Strategies

Incident Response Plan

Having a well-defined incident response plan in place is crucial.

It should include things like:

- Communication protocols
- Containment procedures
- Steps for recovery
- IT contact numbers

Data Backup and Disaster Recovery

Regularly backing up data is a vital component of Right of Boom. Another critical component is having a robust disaster recovery plan.

Forensic Analysis and Learning

After a security breach, conduct a thorough forensic analysis. It's essential to understand the nature of the attack. As well as the extent of the damage, and the vulnerabilities exploited.

Legal and Regulatory Compliance

Robust Access Control and Authentication

Navigating the legal and regulatory landscape after a security breach is important.

PERSONAL & HOME-OFFICE

Titanium Micro Mercury

Introducing the Titanium Micro Mercury External SSD – a pocket-sized powerhouse! Crafted from spaceship-grade titanium, it’s tough, compact, and up to 5x faster than conventional portable HDDs.

Additionally, it features a built-in tracker for added security. The Titanium Micro Mercury External SSD is not merely a storage device, but a sophisticated solution for all your data needs.

PERSONAL & HOME-OFFICE

Smart Home Tech You Should Adopt and Avoid

In the age of smart living, our homes are becoming increasingly intelligent. They’re designed to cater to our every need. Smart gadgets are transforming how we turn on the lights, home security, and more. They even help us feed our pets from afar.

But with the rapid evolution of this technology, it’s crucial to make informed choices. To know what to adopt and what to avoid. Every smart technology isn’t as helpful as another.

You also must be careful of things like security and oversharing.

Here are some tips on what smart home tech to adopt and to avoid.

Adopt: Smart Lighting Systems

Smart lighting systems have proven to be both energy-efficient and convenient. They allow you to control the ambiance of your home. As well as schedule lights to go on and off. You can even change colors to match your mood.

They do this by optimizing heating and cooling based on occupancy patterns.

Avoid: Overcomplicating Security Systems

Robust security systems are essential. But overcomplicating them with unnecessary gadgets may lead to confusion and inefficiency. The more devices you add to a security system, the more exposure for your network.

Adopt: Smart Home Hubs

Smart home hubs are popular. They give you one place to manage all your smart devices and enable seamless communication between them. Investing in a compatible hub ensures a harmonious smart home experience.

Avoid: Ignoring Privacy Concerns

The convenience of smart home tech should not come at the expense of your privacy. Be cautious about

Avoid: Cheap, Unbranded Smart Devices

There is a definite allure to low-cost smart devices. Yet these unbranded alternatives often compromise on security, support, and functionality. This is true for both security and performance.

Investing in reputable brands ensures several benefits.

Including:

- Regular updates
- Security patches
- Compatibility with other smart home devices
- Long-term support

Adopt: Smart Thermostats

Smart thermostats learn your habits. They adjust your home's temperature accordingly. They contribute significantly to energy savings.

devices that constantly record audio or video. Especially if done without clear user consent. Regularly review privacy settings. Limit data collection. Choose devices from reputable companies that focus on user privacy and data security.

Adopt: Smart Home Security Cameras

Smart security cameras provide real-time monitoring and remote access. They also enhance the safety of your home. Look for cameras with features like motion detection, two-way audio, and cloud storage.

Avoid: Impulse Buying Without Research

The excitement of new gadgets can lead to impulse purchases. Before buying any smart home device, conduct thorough research. Read reviews and compare features.

WEBSITES

Securing Your Online Presence: 6 Must-Follow Website Security Tips

With the winter holidays approaching, it's crucial to ensure that your website is secure, especially as online activity often increases during this season. Here are six website security musts for the holiday season:

1. Update and Patch: Ensure that all your website software, including the content management system, plugins, and themes, are updated to their latest versions. Updated software is less vulnerable to attacks.

2. Strengthen Passwords: Encourage or enforce strong password policies for all users, especially for admin access. Consider implementing password expiration policies.

3. Enable Two-Factor Authentication (2FA): Add an extra layer of security by implementing two-factor authentication for logging into the backend of your website.

4. Regular Backups: Set up regular backups of your website. In case of an attack, having a recent backup can mean the difference between a quick recovery and a prolonged downtime.

5. Secure Payment Gateways: Ensure that any payment processing is secure and compliant with the Payment Card Industry Data Security Standard (PCI DSS).

6. Monitor for Suspicious Activity: Keep an eye on your website's traffic and logs for unusual activities that could indicate an attempted or successful breach.

With online activities peaking, your website's security should not be left in the cold.

CONTACT US

CORPORATE

Most Secure Way to Share Passwords With Employees

Breached or stolen passwords are the bane of any organization's cybersecurity. Passwords cause over 80% of data breaches. Hackers get in using stolen, weak, or reused (and easily breached) passwords.

But passwords are a part of life.

Since you can't get around passwords, how do you share them with employees safely? One solution that has gained popularity in recent years is using password managers.

Why Use a Business Password Management App?

Here are some of the reasons to consider getting a password manager for better data security.

- **Centralized Password Management**

A primary advantage of password managers is their ability to centralize password management. They keep employees from using weak, repetitive passwords. And from storing them in vulnerable places.

- **End-to-End Encryption**

Leading password managers use robust encryption techniques to protect sensitive data.

- **Secure Password Sharing Features**

Password managers often come with secure password-sharing features. They allow administrators to share passwords with team members. And to do this without revealing the actual password.

- **Password Generation and Complexity**

Password managers typically come with built-in password generators. They create strong, complex passwords that are difficult to crack.

- **Secure Sharing with Third Parties**

Password managers offer secure methods for sharing credentials with third-party collaborators or contractors.

CORPORATE

PERSONAL & HOME-OFFICE

9 Smart Ways For Small Businesses to Incorporate Generative AI

There is no escaping the relentless march of AI. Software companies are rapidly incorporating it into many business tools.

Leveraging Generative AI, small businesses can unlock a world of possibilities. This includes everything from enhancing customer experiences to streamlining operations.

Here are some smart and practical ways to incorporate GenAI.

1. Personalized Customer Experiences
2. Presentations & Graphics Creation
3. Chatbots for Customer Support
4. Data Analysis and Insights
5. Product Design and Prototyping
6. Supply Chain Optimization
7. Dynamic Pricing Strategies
8. Human Resources and Recruitment
9. Predictive Maintenance

Coolest Smart Gadgets at IFA

Every year, tech enthusiasts eagerly anticipate Europe's most prominent technology trade show. It's the Internationale Funkausstellung Berlin, or simply IFA.

This is a showcase of the latest and greatest innovations in consumer electronics.

The show includes everything from cutting-edge smartphones to futuristic smart home gadgets. IFA never fails to impress.

Here are some of the coolest smart gadgets unveiled at IFA.

- Samsung's JetBot 90 AI+ (intelligent robot vacuum)
- Spatial Reality Display (creates 3D objects)
- Philips Hue Gradient Lightstrip
- Bose QuietComfort 45 Headphones
- LG's Rollable OLED TV (a disappearing smart TV)
- Bosch's Virtual Visor (selectively darkens glare spots)
- TCL Wearable Display (a personal cinematic experience)

CORPORATE

7 Helpful Features Rolled Out in the Fall Windows 11 Update

In a world where technology constantly evolves, Microsoft stands at the forefront. It continues to pioneer innovations. Innovations that transform how we interact with our digital universe.

The fall Windows 11 update is a testament to Microsoft's commitment to excellence. It's more than just an upgrade. It's a leap into the future of computing. Microsoft touts it as "The most personal Windows 11 experience."

Here are some of the great features recently rolled out:

- Microsoft Copilot: Your Intelligent Partner in Creativity
- Updated Apps (Paint, Snipping Tool, Clipchamp & More)
- Easy Data Migration with Windows Backup
- Microsoft Edge: A Better Browsing Experience
- Save Energy & Battery Power
- A More Personal Windows 11 Experience

Technical Framework maintains an **A+** rating with the **BBB**

A+

BBB

FORT COLLINS AREA CHAMBER OF COMMERCE

GREELEY AREA CHAMBER OF COMMERCE