frogworks

Managing Your Technology So Your Business Doesn't Croak.

February 2025

Issue 02 Volume 15

Ribb"IT" Review

Technology: The Backbone of Effective Business Continuity Planning

Getting your business up and running is a challenge, especially when building a new brand from the ground up that must compete with similar long-standing companies. It would help if you advertised to get your target audience's attention and regularly track how your company is doing to ensure success. But when the unpredictable occurs, you must know technology's role in enhancing business continuity planning.

What Is Business Continuity Planning?

When the unexpected happens, you should be ready. That includes when the occasional human error leads to cyber attacks and data loss or when natural disasters and pandemics halt the supply chain and your business.

Business continuity planning means you have emergency plans guaranteeing you can still fulfill supply and demand for all stakeholders and customers. It also means you're readily prepared to uncover, deal with, and survive company disruptions so these events don't force you to shut down permanently.

However, the only way to identify and manage threats of all kinds and properly prepare for their impact is by using technology in the following ways to keep up your obligations, resilience, and competitiveness.

Cont. On Page 2.

This monthly publication provided courtesy of:
Alex Bleam,
Owner of Frogworks

Technology: The Backbone of Effective Business Continuity Planning

Cont. From Page 1.

Technology Offering Disaster Recovery

Let's say your business experiences a massive flood due to a recent storm or broken pipes. Some pieces of hardware, such as physical servers, may feel the effects and refuse to power on, automatically breaking communication plans and processes with customers and suppliers. A business impact analysis can not only help you determine the severity level of damages but also identify scenarios for what to do next.

Once that's done, determine which assets are most critical since they make or break daily activities like proprietary software or customer databases. Fixing these first helps you minimize downtime. However, technology's role in enhancing business continuity planning doesn't stop there. You can use backup servers, or switch to emergency communication channels.

Considering Cyber Security Measures

Unfortunately, it's not just natural disasters that harm a company. Many attackers use phishing efforts, malvertising, and other malicious campaigns to steal personal information, ruin your image, and destroy your company.

By creating strong passwords using multi-step verification or a password generator, you instantly have a stronger line of defense against cyber criminals. Your employees can also undergo cybersecurity training regularly to improve risk management, and as the owner, you can update all programs and devices so they always have the patches they need to avoid vulnerabilities.

Staying Updated with Technological Advancements

5G connectivity is also receiving much praise for its role in business continuity since it promises stronger connectivity that can further your communication plan and faster speeds when uploading or downloading.

Technology's role in enhancing business continuity planning is vast and vital, giving any company a fighting chance under any circumstances. Further research on how it can help yours today!

Hackers Exploit CCTV Camera Flaws

Is your establishment's surveillance system as secure as you think? Gone are the days when these security measures were a set-and-forget solution. Hackers have learned to take advantage of and breach CCTV camera flaws.

How They Do It

The cybersecurity research company GreyNoise discovered these attacks through an advanced AI analysis tool. It found that cybercriminals have targeted network device interface-enabled (NDI) pan-tilt-zoom (PTZ) cameras from various manufacturers.

Their main vector of attack is zero-day vulnerabilities or newly discovered software flaws that have yet to receive a patch. Once accessed, they could manipulate camera settings, watch live feeds, and start botnet integration.

Are Your Cameras Compromised?

Expensive doesn't necessarily mean secure. GreyNoise warns that the affected devices belong to the high-cost category, some worth thousands of dollars.

The list includes PTZOptics, SMTAV Corporation, and Multicam Systems SAS units based on Hisilicon Hi3516A V600 SoC V60, V61, and V63. Get firmware updates immediately if you have these setups with anything lower than the 6.3.40 version.

Message your provider to confirm the status of your specific cameras for your peace of mind.

Cont. On Page 4.

Hackers Exploit CCTV Camera Flaws

Cont. From Page 3.

Signs You Have Hacked Cameras

Aside from updating your system and reading communication from your provider, it never hurts to check for unusual activity:

- The camera emits strange sounds or unfamiliar voices
- Unexpected movements or angles during a recording
- LED light blinks or flashes despite nobody accessing the camera
- Changed settings without your input

An unexplained spike in data usage or network traffic

Minimizing Cyberattacks

Why wait for your establishment’s security to become compromised? Stay proactive through:

- Stronger passwords: Some use their model’s default username and password and forget to change them later. Hackers ping every internet-capable device to find easy targets, so pick a random combination of upper-case and lower-case letters, numbers, and special characters.
- Limited access: Attackers can access individual authorized devices instead of the entire network. Try to minimize the number of devices that can manipulate the security system.
- Virtual private networks (VPNs): Do your operations require remote camera access? Get a VPN to hide the connection and make your traffic more private.
- Cloud access: If you can’t set up a VPN, cloud-based usage is the next best option. A heavily monitored third-party server hosts device control and recorded footage.
- Built-in advanced data encryption: Look for cameras with technologies like SSL/TLS and WPA2-AES that make it harder for hackers to access footage and other data. It’s like adding another lock to your digital door.
- Two-factor authentication (2FA): Many cameras already have 2FA, which requires an extra step when logging in; you just have to enable it. Even when someone cracks your password or exploits CCTV camera flaws, they still need your approval to get in.

We Have an E-Newsletter!!!

Do we have your e-mail address??? If you would like to receive our newsletter though email please visit us at:

www.getfrogworks.com/newsletter