# LABEOC

## Louisiana Business Emergency Operations Center

**February 18, 2026**

As we have mentioned in previous newsletters, cybersecurity is not a one-time effort; it requires constant vigilance. Larger organizations may employ a dedicated team to keep their networks secure, while smaller businesses might choose to outsource this responsibility. This month's article isn't designed to turn you into an expert, but to equip you with the tools to ask better questions of your managed service provider (MSP), thereby enhancing your security. It may sound cliché, but in cybersecurity, it's often like running from a bear. You don't have to be faster than the bear—just faster than those around you. In cybersecurity, make yourself a harder target, and the attackers will likely move on to easier prey.

This month, we will discuss a strategy that can help bolster your organization's defenses: edge devices. Most businesses tend to think of cybersecurity in terms of laptops, email security, and antivirus software. While these are important, they are not the first line of defense against the internet. That role belongs to your edge devices, which act as a boundary between your internal network and the outside world.

In practical terms, edge devices are the systems that route traffic, enforce security policies, and enable remote access. The **Cybersecurity & Infrastructure Security Agency (CISA)** describes edge devices as critical components that serve as security boundaries between internal enterprise networks and the internet. Common examples of edge devices include enterprise routers, firewalls, and VPN concentrators.

You might be wondering, "What about our edge devices?" The issue is that maintenance of edge devices is often overlooked. Keeping laptops and desktops updated takes considerable time and attention, and edge devices are sometimes considered "working fine, so we hesitate to risk breaking them" when updates are needed.

However, attackers are aware of this tendency. Edge devices sit at the network boundary, are often exposed to the public internet, can be challenging to monitor effectively, and, if compromised, can grant access to the rest of the network. So, what steps can you take to make your organization harder to breach? Here are some quick actions every business can implement:

1. **Inventory all network equipment**: Physically check each device to ensure you and your MSP know who owns it and who is responsible for its maintenance.
2. **Questions for your MSP**: Inquire about when the edge devices were last patched or upgraded. Have any of them reached the end of their life cycle? This doesn't mean they are unusable, but rather that the manufacturer has stopped issuing updates and patches for vulnerabilities.
3. **Eliminate unnecessary internet-facing admin portals**: If you or your team do not need specific capabilities, ask your MSP to remove them.
4. **Strengthen admin authentication**: Ensure that your admin authentication is as robust as your user authentication, especially if you are using multi-factor authentication for your admin team or MSP.
5. **Backup, backup, backup**: Make sure you are adhering to the 3-2-1 backup strategy—three backups, in two different formats, with one kept off-site. Ask your MSP or IT team when they last tested the backup to confirm that it works.

By following these steps, you can enhance the security of your network and make it more challenging for potential attackers.

Jim

**James 'Jim' Williams**
Public-Private Partnership Operations Officer
LABEOC at the NIMSAT Institute
University of Louisiana at Lafayette
james.williams@louisiana.edu
337.482.0633

# GOHSEP Academy at UL Lafayette
# Spring 2026 Dates

**Free and open to the public!**

**REGISTER NOW**

**March 5-6**
**Benefit Cost Analysis**

**March 18 - 19**
**Evacuation, Sheltering, and Re-entry**

**March 25 - 26**
**Stronger Standards, Safer Homes**

**April 1-2**
**Public Assistance – Debris Removal**

-

**April 29-30**
**Hazard Mitigation and Assistance Grants**

**Location**
Abdalla Hall Auditorium
University of Louisiana at Lafayette
635 Cajundome Blvd.
Lafayette, LA 70506

**Time** (Classes follow a two-day format)
Day 1: 12:00 pm - 4:00 pm
Day 2: 8:00 am - 12:00 pm
Register at https://stems.gohsep.la.gov/

***Hosted by***

GOVERNOR'S OFFICE OF HOMELAND SECURITY & EMERGENCY PREPAREDNESS
GOHSEP
NIMSAT NATIONAL INCIDENT MANAGEMENT SYSTEMS AND ADVANCED TECHNOLOGIES
LA BEOC LOUISIANA BUSINESS EMERGENCY OPERATIONS CENTER
LEPA

Register here

## Preparedness Resources

Ready
Prepare. Plan. Stay Informed.

GETA GAME PLAN

emergency
LOUISIANA.GOV

## Website Links

Latest News

Helpful Links

Register

Follow us for the latest news!

The LABEOC is managed by the National Incident Management Systems and Advanced Technologies Institute at the University of Louisiana at Lafayette, in partnership with the Governor's Office of Homeland Security & Emergency Preparedness and Louisiana Economic Development.