WYRE Technology

How to Troubleshoot
the Most Common Network Errors

wyretechnology.com

sales@wyretechnology.com

423-874-8230

Table of Contents

Introduction 3

Weak Wi-Fi Coverage 4

a) Your APs Are Undersized 4

b) The Nearest AP Is Too Far Away 5

c) Your Components Need Updates 6

Older Components 7

Why Companies Use Legacy Systems 9

Problems with Legacy Systems 9

How to Migrate from Legacy Systems 10

User Education 11

The Five Main Types of Breaches 12

The Four Main Types of Incidents 13

How to Protect Your Network from Breaches and Incidents 13

Lack of Network Segmentation 15

Conclusion 16

Introduction

Every network shares similar challenges. Below are three issues you're likely to encounter, along with their solutions. Be sure to check out the bonus tip at the end!

Weak Wi-Fi Coverage

Have you ever been in the middle of an online meeting and watched in confusion as the image on the screen starts to fragment or the person's words go out of sync?

If this happens with most meetings, most times, then it's likely your Wi-Fi signal isn't strong enough to handle the load from your network.

Wi-Fi begins at an access point, or AP.

An AP allows other wireless devices to connect to a wired network. The AP then gives all the devices connected to it access to the outside world (i.e., the internet).

If your Wi-Fi signal is weak, the nearest AP is a good place to start troubleshooting.

a) Your APs Are Undersized

The number of devices on your Wi-Fi network matters. The more devices, the higher the demand.

For example, a bakery with two desktop computers, two payment devices, and one printer would need a simple, straightforward network.

On the other hand, a hospital with thousands of devices would have to scale up in a serious way to include dozens of segmented networks and an array of components.

If your business has grown since your network was installed, it's time to take a fresh look at your components—including any APs—and make sure they're still the right fit.

Remember: having the right components for the size of your business helps more than just the Wi-Fi *signal*. It can also improve stability and security.

b) The Nearest AP Is Too Far Away

Walls, closets, cubicles, metal, other Wi-Fi devices, even water coolers—all of these can cause a drop in your Wi-Fi signal quality. Be sure APs are well-placed to provide service to the necessary areas and are kept away from obstacles that might cause interference.

If you're a small-to-medium-size business, look into an affordable, high-performance product like Ubiquiti's U6 line of APs, all of which can be ceiling-mounted, providing a clear path for your Wi-Fi signal.

c) Your Components Need Updates

When was the last time the firmware on your network components was updated? Manufacturers provide downloadable updates at regular intervals, and if the updates aren't installed, not only will your components not work as well, but they also may be vulnerable to cyberattacks. In fact, according to a survey conducted by Microsoft, in 2021 over 80% of global enterprise businesses reported firmware cyberattacks.[1]

Installing firmware updates is simple (though it's best to perform the installation after a full backup and when the least amount of users will be affected). Again, check with your product's manufacturer for instructions.

d) Your Components Need Up*grades*

How old is your router? Your switch? Your AP? What is the state of the wiring that connects them?

If you're still using the same computer components from five years ago, they're probably in need of replacing.[2] Technology moves fast.

Curious about how easy—or not—it is to upgrade older components? Keep reading!

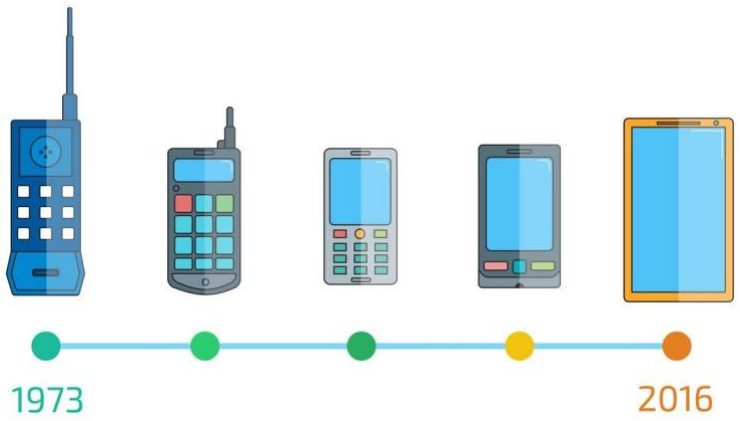
[1] https://www.bbc.com/news/business-56671419

[2] https://www.lifewire.com/how-long-do-routers-last-5074393

Older Components

If your company has been around awhile, you're probably familiar with the term *legacy*.

In computing terms, *legacy* refers to older, outdated, no-longer-supported software and hardware that's still in use by a company.



As you can imagine, legacy systems have their downsides. In 2020, technology market researchers Vanson Bourne conducted a survey called "The State of Data Management." They spoke with 500 IT decision-makers in both the US and UK. When discussing legacy environments, 88% said their business had experienced "challenges trying to load data into data warehouses [management systems for data[3]]." One of the biggest reasons for the challenges? Legacy technology.

And for 49% of the survey's responders, legacy systems were "restricting data movement and the loading of data into a data warehouse."[4]

[3] https://www.oracle.com/database/what-is-a-data-warehouse/

[4] https://www.snaplogic.com/resources/research/the-state-of-data-management/thankyou

Difficult moving and managing data is bad enough, but perhaps the biggest downside to a legacy system is its vulnerability to cyberattacks.

Security patches for out-of-date software and hardware don't exist—when the equipment is stamped as "end of life," or EOL, companies stop supporting it. This gives cybercriminals an easy target. In 2020, Rangely District Hospital in Colorado was targeted by a ransomware attack. The breach may have included confidential patient information, such as social security numbers, driver's license numbers, health insurance details, and even diagnoses.[5]

The attack targeted the hospital's legacy software system, leaving staff unable to view patient records.[6]

In 2020, Adobe-owned e-commerce platform Magento was targeted by cybercriminals. Using malicious code, they stole customer credit card information.[7] The malware infected 8,170 stores across all platforms, and "82% of stores that had malware were running an unsupported version of the product."[8]

Magento's legacy software was out of date by only a few *months*.

[5] https://www.theheraldtimes.com/rdh-suffers-ransomware-attack/rangely/

[6] https://www.hipaajournal.com/ransomware-attacks-reported-by-rangely-district-hospital-and-electronic-waveform-lab/

[7] https://www.zdnet.com/article/magento-online-stores-hacked-in-largest-campaign-to-date/

[8] https://business.adobe.com/blog/the-latest/secure-your-storefront-enhanced-magento-security-scan-tool

Why Companies Use Legacy Systems

Even with all their potential problems, legacy systems are used for a reason—several, actually—especially by established businesses.

a) **Legacy systems can be critical to a company's IT infrastructure**. Banks use legacy environments to process transactions and manage accounts. Branches of the US government, like the IRS, are steeped in legacy systems.[9] And retail merchants report spending "58% of their IT budget to maintain legacy systems."[10]
b) **Legacy environments are familiar**. They've been in use for a long time, so staff know exactly how to finesse the systems to get what they need.
c) **Legacy products seem cost effective**. After all, you're simply paying for upkeep, right?

Not quite.

Yes, upgrading a legacy system can be costly: new products and equipment, installation, licensing, plus training staff to use the new system.

But *not* upgrading brings its own set of problems.

Problems with Legacy Systems

- **Parts for legacy systems are expensive**. According to the US Government Accountability Office, "Ten critical federal information technology (IT) legacy

[9] https://www.treasury.gov/tigta/auditreports/2020reports/202020044fr.pdf

[10] https://www.retailtouchpoints.com/resources/retailers-spend-58-of-their-it-budget-on-legacy-system-maintenance

systems . . . ranged from about 8 to 51 years old and, collectively, cost about $337 million annually to operate and maintain."[11]

- **Recruiting support is difficult**. Finding specialists familiar with legacy systems can be challenging, not to mention costly.
- **Legacy systems use more power than modern systems** and, therefore have a bigger carbon footprint.[12]
- **Legacy equipment is slow**. In fact, since 2013, supercomputers have increased in speed by 40% *every year*.[13]

How to Migrate from Legacy Systems

Moving away, or migrating, from a legacy system may not be as difficult as you think. There are two main paths: **transformation** and **lift-and-shift**.

Lift-and-shift moves your network's software and data to a cloud or hybrid-cloud service—with little-to-no redesign.

Transformation, or modernization, slowly and methodically brings your network software and hardware up to date with current technology.

No matter which path you choose, it will take time and planning. It *is* possible, however. The details will need to be worked out by your CIO and technology team. If you're a small business, or if you don't have in-house IT staff, contact your local managed service provider (MSP), for help.

[11] https://www.gao.gov/products/gao-21-524t

[12] https://www.aboutamazon.com/news/sustainability/reducing-carbon-by-moving-to-aws

[13] https://www.datacenterknowledge.com/supercomputers/after-moore-s-law-how-will-we-know-how-much-faster-computers-can-go

User Education

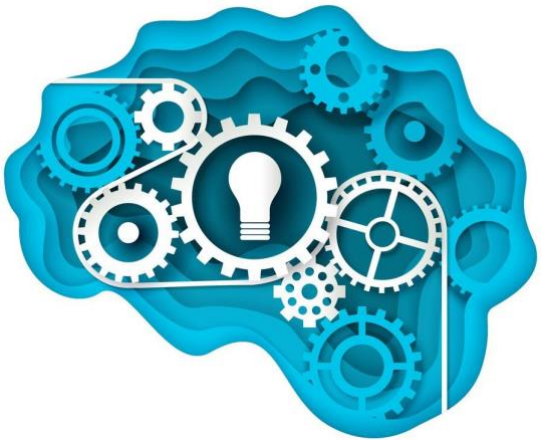
In 2021, data breaches reached a record high.[14] Identity Theft Resource Center, or ITRC, found that the number of breaches rose by 23% over the previous year.[15] And according to IBM, the cost for a data breach in 2020 averaged $3 million.[16]

Averaged—meaning there were breaches that cost companies even more.

Remember the Colonial Pipeline ransomware attack? Cybercriminals stole *one* password.[17] They then charged the company nearly $5 million to recover the stolen data.[18]

Whether a network is business or personal, it's only as safe as the people who look after it. According to IBM's "Cost of a Data Breach Report 2020," preparing for an incident "was the highest cost saver for businesses." The actual savings? Around $2 million.

Preparation begins with **education**, so let's get started.



[14] https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/

[15] https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises

[16] https://www.ibm.com/account/reg/us-en/signup?formid=urx-46542

[17] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

[18] https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html

The Five Main Types of Breaches

- **Social engineering** tries to "trick someone into revealing information (e.g., a password) that can be used to attack systems or networks" (National Institute for Standards and Technology).[19] These "tricks" come in the form of targeted downloads, links, or pleas for help (remember the African prince who wants to wire you money—but first needs access to your bank account?). In its "DBIR: 2021 Data Breach Investigations Report," Verizon found that "85% of breaches involved a human element."[20]
    - **Phishing** is a form of social engineering in which a cybercriminal pretends to be a trusted source in order to acquire credentials, like your username and password. Credentials accounted for 61% of breaches in 2021.[21]
- **Malware** is "malicious code" on your computer or network "with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system" (NIST).[22] Malware includes ransomware like the one used in the Colonial Pipeline attack described above.
- **Web-application attacks** target web-based software, looking for specific data or using the application in a malicious way. In 2021, over 55% of incidents used web applications as their method of attack.[23]
- **Brute-force attacks** are attempts by cybercriminals to hack into a computer system via trial and error, hacking software, and various other methods. It's unsophisticated, but it works.
- **Errors** are simply that: unintentional mistakes that compromise the safety of a computer or network. This includes misconfiguration, misdelivery, and programming errors, and makes up a surprising amount of breaches, at almost 20%.[24]

---

[19] https://csrc.nist.gov/glossary/term/social_engineering

[20] https://www.verizon.com/business/resources/reports/dbir/

[21] https://www.verizon.com/business/resources/reports/dbir/

[22] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf

[23] https://www.verizon.com/business/resources/reports/dbir/

[24] https://www.verizon.com/business/resources/reports/dbir/

The Four Main Types of Incidents

The three most common terms you'll see when reading about **incidents** are the same as above: social engineering, malware, and web-application attacks.

A fourth also exists: **denial-of-service attacks**. DoS attacks take down your computer or network, denying you access. According to Verizon's "DBIR: 2021 Data Breach Investigations Report," DoS attacks have increased over the years and are now the most common incident. Thankfully, they're also the easiest to prevent (more on that in a minute).[25]

How to Protect Your Network from Breaches and Incidents

Every computer network should:

25 https://www.verizon.com/business/resources/reports/dbir/

- **Use strong passwords** on all of its devices, applications, and accounts.
- **Install a firewall** to monitor incoming and outgoing activity.
- **Keep all applications up to date** (updates typically include fixes for known security issues).
- **Install antivirus software** and update it regularly.
- Make sure **downloads come only from trusted sources**.
- **Don't click on links inside emails**. Instead, search for the site or information yourself via a safe search engine like Google.

The larger your network, the more layers of security you need. This means using the skills of an internal IT team or outsourcing.

Time for an added bonus! The fourth most common business computer network issue . . .

Lack of Network Segmentation

Segmenting a network divides it into separate sections. This is accomplished via **switches**. A **switch's** job is to allow multiple devices—from printers to servers to tablets—to see and talk to each other.

Network segmentation is an important—and often overlooked—way to protect your network from cyberattacks. When the network traffic, or data, is isolated between segments, with firewalls for added security, those segments become your front line of defense against outside cyberattacks. How? Cybercriminals who sneak through the first line find it harder to get through the second.

Different security rules can even be created for each segment, ensuring each group of users has only the permissions they need to do their job. This helps contain malicious attacks and can prevent untold amounts of damage.

Conclusion

As you can see, no matter the size of your network, there will always be issues, from outdated components to cyber vulnerabilities. This means *every* network needs some kind of support. After all, you likely already wear a number of hats. IT doesn't have to be one of them.

If you don't currently have an in-house IT team, research managed service providers, or MSPs, in your area. If you're in Chattanooga, Tennessee, or anywhere else around the world, please feel free to give WYRE Technology a call at (423) 874-8230. We always help!