Frontier BUSINESS™

# Security Is One Thing. Confidence Is Another.

A SECURITY EBOOK.

# Imagine this.

It's 4:30 on a Friday afternoon and you receive a frantic call from a security systems administrator: An unauthorized third party has accessed your company's cloud, and the data on it may have been leaked.

It's not just *your* network and data at risk—it's the information that belongs to your users, subscribers, and employees. Losing or compromising it could be catastrophic—and the cost could be crippling.

**Worst of all, you don't have a plan in place to fix it.**

There's no such thing as over-preparing for a security incident. If and when one strikes, you need tools to mitigate its impact. It's important to establish processes and points of contact for every aspect of security planning, preparation, and deployment.

With today's "always-on" connectivity, you could be overlooking all the areas for possible vulnerability. Let's explore some common security issues, how to address them, and what it takes to heighten your own security measures.

The average total cost of a single DATA BREACH: $3.62 million.[1]

[1] Ponemon Institute, "2017 Cost of Data Breach Study."

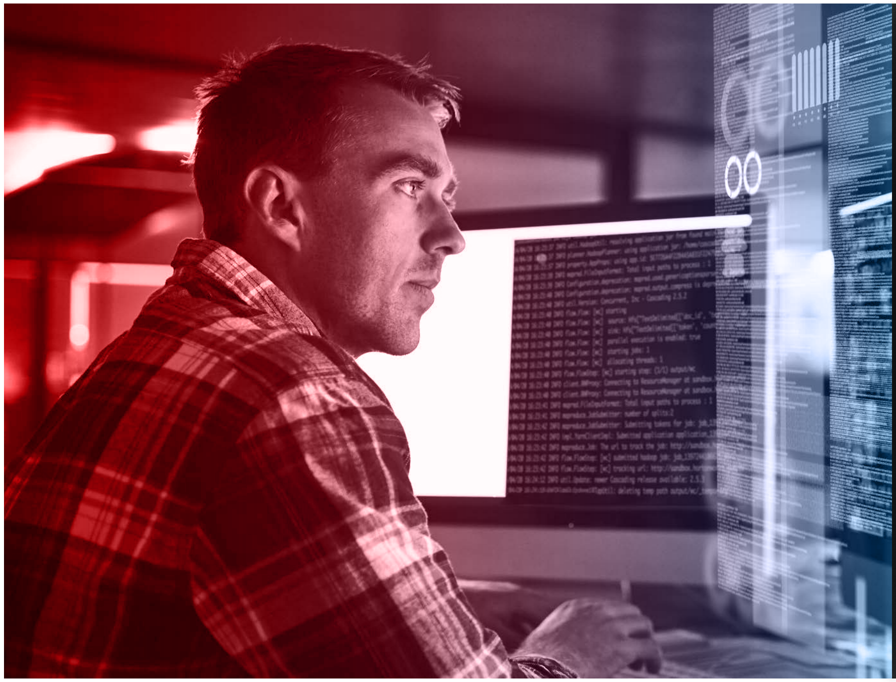
# Redundancy vs. Resiliency

## FIRST THINGS FIRST, LET'S FIGURE OUT YOUR SECURITY DESIGN.

If you have too much security (redundancy), that's not necessarily a bad thing—but sometimes multiple iterations of identical backups can slow you down when you're in the middle of a security crisis. A redundant network is multiple versions of the same exact information—you've crossed your t's and dotted your i's, but you've done it to the same letter a whole lot of times. On the other hand, a resilient network allows you to very quickly identify—and, more importantly, isolate—a security incident. That means while your experts are fixing the vulnerability, the rest of your organization can keep plugging away without interruptions.

At some point, identical versions of the same data backup—as helpful as you think they may be—just get in the way, and they slow you down. Identify when too much of a good thing becomes overkill, and work to adopt a nimbler approach.

Once you've identified whether your security design is redundant or resilient (or maybe a hybrid of both!), you can start looking more closely at specific technologies and solutions to see how their security stacks up.



RESILIENCY QUICK TIP:
Avoid one-size-fits-all NETWORK SECURITY; there's really no such thing. Take a tailored approach so you know your specific needs will be satisfied.

# VoIP Security

## NOT ALL PHONE CONNECTIONS ARE CREATED EQUAL.

If you're just talking about the connections within your four walls, VoIP is actually fairly locked down. But if you connect to the rest of the world—and as a growing company, of course you are—where the security issue comes in is with those communications. Other organizations' networks could be putting your own in jeopardy.

VoIP traffic is susceptible to many of the same threats broadband networks are—even down to the type of attack. So, yes: Spoofing, spamming, and phishing can all occur over phone calls. For example, a user's caller ID could falsely indicate a call is coming from a seemingly "safe" individual or entity. Attackers use these calls to mine personally identifying information (PII), financial information, or other pieces of data they could use to further harm the target.

So, require your employees to exercise the same caution over the phone that they do when they encounter questionable emails or online forms. Make sure your connections are always secure, and that your security software is updated with the latest patches and fixes.

VOIP SECURITY QUICK TIP

Make absolutely certain all your VOIP calls are conducted on a secure network.

# Cloud Security

## KEEP YOUR DATA IN THE CLOUD, BUT GET YOUR HEAD IN THE REAL WORLD.

Access to the cloud has changed the way we work. But, it also makes you more vulnerable to risks associated with having sensitive data stored where attackers could find it. And while it's great news that you no longer have to carry around a flash drive (or floppy disk!) that holds your most important files, the ugly flip side is that without proper security measures, those files on the cloud are far more vulnerable than their physically stored predecessors.

You don't always know how, when, and where your employees are connecting to the cloud. So make sure you have sophisticated security measures in place to prevent them from accessing confidential information over a public Wi-Fi network, for example.

CLOUD SECURITY QUICK TIP:

Require all users to use a VPN to access your CLOUD.

# BYOD Security

## BRING YOUR OWN DEVICE–NOT YOUR SECURITY VULNERABILITIES.

There's no way to stop people from using their personal devices to access organizational information. And the number of device types they're using may make it frustrating to ensure everyone's following the rules. But multiple device use is inevitable, so you need to keep up with security concerns.

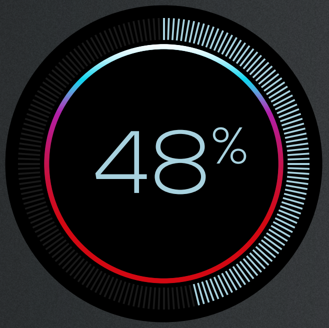
Some red security flags where BYOD is concerned: people installing malicious apps or spyware on their phones, connecting to unsecured public networks, using "jailbroken" phones that don't comply with their original operating systems, or experiencing loss or theft of personal devices.

Explore BYOD solutions that protect against the manifold security threats that could compromise your data while people are working remotely or using their phones for sensitive business. You'll have to consider many different technologies and platforms, but not having these measures in place is simply not worth the risk.

# Keeping your employees educated.

## MAKE SURE EVERYONE'S SAFELY UP TO SPEED.

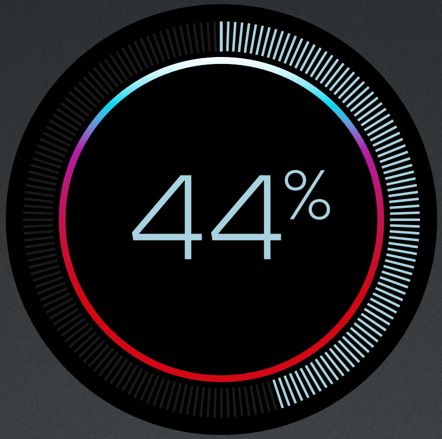
Every single one of your employees needs to be held accountable when it comes to upholding a safe network environment. Make your rules cut and dry; over-define policies so there's no room for misinterpretation. All employees need to be trained on your security measures–and so do your agencies, vendors, partners, and contract or temporary workers.



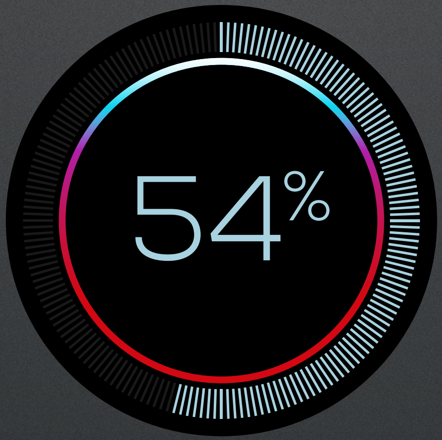
48% OF ORGANIZATIONS REPORTED THEY DID NOT HAVE AN EMPLOYEE SECURITY AWARENESS TRAINING PROGRAM.[2]

BYOD SECURITY QUICK TIP:
Educate employees on the dangers of "JAILBREAKING."
Your corporate data is unsafe–but the same goes for their personal information.

[2] PwC, "The Global State of Information Security® Survey 2018."



44% OF EXECUTIVES SAID THEY DID NOT HAVE AN OVERALL INFORMATION SECURITY STRATEGY.[2]



54% DID NOT HAVE AN INCIDENT RESPONSE PROCESS.[2]

# Take the right precautions.

## THERE'S NO SUCH THING AS BEING TOO PREPARED.

It's common to operate under the assumption of "it won't happen to me." When it comes to something as essential as confidential information getting into the wrong hands, that's a bad mentality to have.

If a security incident strikes, being as prepared as possible means you'll have the tools in place to mitigate impact. Establish processes and points of contact for every aspect of security planning, preparation, and deployment. You need a strategic, quick, resilient solution that allows you to identify, isolate, and eliminate an issue, without shutting down your entire enterprise.

Tailor the way you prevent against and handle potential issues to ensure your business doesn't slow or stop when something dangerous strikes. Put the right team members in place to build a plan, and come up with solutions that are issue-specific rather than one-size-fits-all.

And if you can't do it all, don't worry. Consider outsourcing some of your security oversight and maintenance. There's no such thing as too much coverage.

[2] PwC, "The Global State of Information Security® Survey 2018."

## RISK ASSESSMENT

Evaluate your current state. Ask employees on the security front lines to prepare a report that lists vulnerabilities, as well as opportunities to beef up safety measures. Some questions to ask include:

+ Why is this a danger to our organization?
+ Are we using anything to address it now?
+ What kind of data could be compromised?
+ How many people would a breach affect?
+ What are the tools we'll need to remedy this?
+ How soon can we fix it?

## CRISIS MANAGEMENT STRATEGY

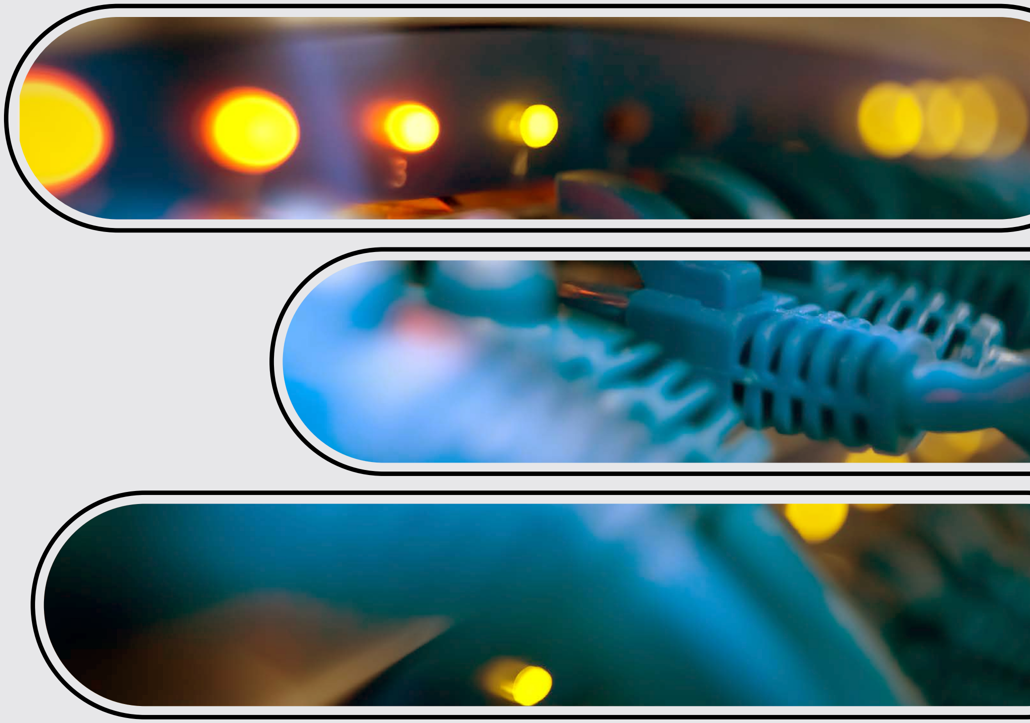
Sometimes, even with the right security measures, you're going to experience a data breach. You need to have a strategy ready; otherwise, you risk worsening the severity of the attack because you weren't prepared. Things to think about as you're building your strategy include:

+ Have we identified the specific target, and has it been isolated?
+ Can we determine who did it, and how they got in?
+ Was other data compromised?
+ Who does this affect?
+ Who needs to know about this?
+ How are we going to communicate it?
+ Can we figure out how long this will impact us?

## DATA BACKUP AND RECOVERY

One of the most critical components when you're moving forward from an attack is a robust backup of the data you had prior to it. Your backups should be comprehensive, automatic, and constant. Here are a few more things to consider when you're assessing your backup and recovery technology:

+ Is this stored in a cloud location totally separate from all my other data?
+ What are the steps we need to take to recover lost data?
+ Do I know how long it will take to recover?
+ Are there people who are constantly testing our backup and recovery solutions?



# It's time to get going.

## IT'S NEVER TOO EARLY TO START THINKING ABOUT NEXT STEPS.

It may seem daunting to begin an honest assessment of how in danger your networks actually are, but every moment you waste is another opportunity for devastating consequences. Start taking stock of your security measures today, and take action to make some big changes—so that when an attacker is ready to strike, you won't be a target.

Frontier BUSINESS℠ | *Isn't it time your business was Custom(er) Fit℠?*

VISIT business.frontier.com/enterprise