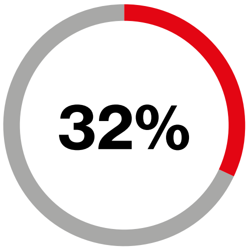
Point of view

3 simple rules to improve your cybersecurity.

Just because you're not a multi-million-dollar business doesn't mean that you aren't a big target for cybercriminals. The good news is that you don't need a huge budget or team of IT specialists to keep data and systems secure. But you do need to be smart about how you prioritize your time and money. We've got three suggestions to help.



Our Mobile Security Index analysis found that almost a third (32%) of organizations admitted to having sacrificed mobile security to improve performance.

Know when to let go

Information is crucial. Gathering the right data can help you serve customers better and grow your business. But are you guilty of hanging onto data that's no longer useful? If so, you could be exposing yourself to greater risk – even if it's of no value to you, crooks could still use this data to further their dastardly plots.

Knowing when to let go can be hard, but here are some tips to help you decide what you need to get rid of.

Dump data you don't need

Resist the temptation to horde data. Securely dispose of any that is no longer relevant to your current or anticipated business needs. If you don't store it, it can't be stolen. Old customer lists? Ditch them – or a cybercriminal could get hold of your customers' sensitive data.

This includes employee data too

Review your employee records too. In this year's Data Breach Investigations Report, we saw a spike in breaches of W-2 data. Cybercriminals can use this to commit identity fraud – and that's not going to be popular with your staff. Again, make sure that you're only storing the data that you need. And if you put employee information into an online tool, make sure it can be accessed only over a secure connection..

Dispose of devices carefully

Always securely erase all data and remove any network connections before recycling devices. Choosing devices with a remote lock and wipe feature will enable you to do this even if you don't have access to the device. A device management solution can help you implement and automate security policies like this across multiple platforms.

Set yourself achievable goals

Our Mobile Security Index analysis found that almost a third (32%) of organizations admitted to having sacrificed mobile security to improve performance. They were then 2.4 times as likely to suffer data loss or downtime related to a mobile device incident. But you don't want to stop employees working from home, or accessing business data on the go. Follow these tips and you shouldn't have to:

Limit devices to networks you trust
You want to let employees work from home and when on the move, but public Wi-Fi could expose your data and systems to additional risk. It may be convenient, and cheap, but it's often unsecure and so just isn't worth the risk. 4G LTE offers a reliable way to stay connected, and we offer a range of affordable voice and data plans to cover all your devices.

Manage your devices
Protect every device with a Mobile Device Management (MDM) solution. These can help protect your devices, even when connecting to open, public networks. Plus, some have added security features that help detect, block and remove a wide range of threats from devices.

Introduce acceptable use policies
Introduce acceptable use policies, including rules for employee-owned devices. In this year's Mobile Security Index, 76% of organizations that allowed employee-owned devices ranked them as one of their top three security concerns.

Stop employees cutting corners
Reduce the temptation for employees to cut corners. If your internet service is not providing the performance employees expect they may get sloppy and look for other ways to connect. It may make their lives a little bit easier, but could pose a big problem for your business. Reduce this risk with Verizon's Internet Dedicated services, available in a range of sizes to suit your business now and as it grows.

Keep calm and carry on

Not all cyberattacks are about stealing data, they can also cause business disruption–most commonly in the forms of Denial of Service (DoS) or ransomware – both featured prominently in this year's Data Breach Investigations Report. These attacks may take systems offline, encrypt or destroy data, or put apps out of use. But it's not just apps that you need to worry about. What would your business do if you lost phone service or couldn't access your premises? You know that even a few hours of downtime can have a big impact on your bottom line. This may sound scary, but there are a number of simple things you can do to improve your defenses.

Back up your data
Protect your business from data loss and downtime caused by ransomware, physical threats like theft and fire, and other threats by backing up your data in the cloud. If something should go wrong, you'll be able to restore data and get operations back up and running quickly.

Block harmful traffic
Shield your network from malware, phishing and ransomware with DNS Safeguard. It's our cloud-based security platform that can be your business's first line of defense against internet-based threats. It automatically blocks your computers and other devices from accessing malicious sites and content. Plus, you're able to enforce company-wide internet policies with customized content blocking.

Protect your communications
If you lose power our Voice over Internet Protocol (VoIP) services can automatically reroute to another number. And you can make calls and manage your settings from any computer connected to the internet. So even if the roads are closed you can still be open for business.

Get the the tools you need

Effective cybersecurity doesn't have to be complicated or expensive. Verizon understands the challenges your business faces and has a range of products built with you in mind, no matter your size. Give your business the protection it deserves and get started today. To learn more, contact your Verizon account representative or have us contact you.

verizon.com/business

verizon✓ business ready