

SPECIAL REPORT | OCTOBER 2026

Executive Summary

A business phone system can be used to make calls that nobody in the business authorised. If an extension, voicemail or administrative account is compromised, calls may be routed to expensive destinations and charges can accumulate before the next invoice arrives. The exact exposure and responsibility depend on the service, its configuration and the contract.

Start with a call to your provider: establish which destinations are enabled, who can change settings, what alerts and limits exist, and who responds after hours. Restrict unused destinations and accounts, protect access, and review unusual call patterns. A spending alert is useful only if someone can act on it; a hard limit must be tested and may interrupt legitimate calls.

This report builds on our earlier guides to the customer call journey and the office devices a cybersecurity policy can overlook. It focuses on a different question: whether your phone system can be misused to generate calls and charges that your business did not authorise.

01 How the charges can arise

A phone system may include handsets, a cloud PBX, a local PBX, voicemail, a provider portal and mobile or desktop calling apps. The configuration differs by business. An attacker who obtains a usable password or exploits an exposed system may be able to place calls or change forwarding rules. Weak credentials, unused extensions that remain active and unmanaged remote access can increase exposure.

A fictional example: a 12-person office closes on Friday. An unused extension is still enabled and has a weak credential. Unauthorised calls are made over the weekend. On Monday, the owner notices an alert and calls the provider. The amounts, response and contractual treatment would depend on the system and agreement; this example illustrates why waiting for a monthly invoice can be too late.

A displayed business number can also be spoofed by a third party. That does not by itself prove that the business phone system was accessed. Ask the provider to investigate call records and account activity before drawing a conclusion.

The distinction matters when a customer calls to complain about a suspicious call appearing to come from your number. Record the time, number and what the caller reported, then pass the details to your provider. Avoid assuring the customer that your system was compromised or that it was definitely secure until the investigation has established what happened.

02 Know what is normal

Review the last two or three months of itemised call records with your provider. Note normal calling hours, destinations, extensions and spend. Identify international and premium-rate calls the business actually needs. A legitimate peak, a new customer or a staff member working late may explain unusual activity, so investigate rather than assume fraud.

Confirm how quickly records are available, whether alerts are real time or delayed, and whether charges can continue before a threshold is detected. The invoice is a useful reconciliation tool; it is not necessarily an early warning system.

Look for patterns that do not fit the way your business operates: calls from an extension assigned to a former employee, repeated calls to a destination you do not recognise, or a concentration of calls outside normal hours. Check whether those calls could be explained by an authorised staff member, an approved forwarding rule or a change in operations. A single unfamiliar number is a reason to check, not proof of fraud.

For a small team, a simple monthly check can be enough to establish the baseline: ask the provider for an itemised report, compare total spend and destinations with the previous month, and nominate someone to investigate exceptions. Add a check after a new site, extension or calling plan is introduced. Ask whether a separate alert can reach the responsible person sooner when activity changes sharply.

03 Put practical limits in place

- Ask the provider to block international, premium or other high-cost destinations that the business does not need. Agree a controlled process for temporary exceptions.
- Set appropriate alerts and, where available, spending or call limits. Confirm whether a limit is a warning or an automatic block, what it covers and whether it resets.
- Use unique strong credentials for administrators and extensions; enable multi-factor authentication for the management portal where supported. Remove unused users and change access when people leave.
- Review voicemail PINs, call forwarding, remote access and who can create or change extensions. Ask the provider to remove default credentials and restrict management access.
- Assign one person and a backup to receive alerts, including after hours. Keep a verified support number accessible when the phone system is unavailable.

Ask the maintainer to keep supported PBX software and firmware updated, review exposed services and restrict remote administration. The right configuration depends on the system and should be checked by the responsible provider.

Controls differ across providers and platforms. Ask which settings are available, who implements and maintains them, and what service interruption could result. Test agreed limits with the provider before relying on them. No single control guarantees prevention.

A restriction should reflect the business. An exporter may need calls to a small number of overseas customers; an office that only calls locally may not need international access at all. Where the system allows it, a provider may be able to limit access to particular extensions or destinations. Agree who can approve a change, when the permission expires and how it will be removed. If a needed feature cannot be restricted in that way, discuss the alternative controls and their limits.

Consider the people behind the settings as well as the technology. A manager who receives an alert while on leave cannot respond, and a shared administrator account makes it harder to establish who changed a rule. Record a primary contact and a backup, review their details when staff change, and make sure both know how to reach support.

04 Read the contract before an incident

Ask for a plain-language explanation of call charges outside the package, fraud monitoring, exclusions, limits and the process for disputing charges. “Unlimited” should be read alongside its fair-use rules, included destinations and exclusions. Do not assume that a monitoring service is insurance or that a provider will automatically absorb fraudulent charges.

Record who owns the portal, PBX, handsets and internet connection, and which supplier will investigate each part. Ask whether monitoring is included, optional or billed separately, and how quickly support can block traffic outside office hours.

For example, the business may have one company providing internet, another hosting the PBX and a third maintaining desk phones. A fault can otherwise pass between them while calls continue. Keep a short contact sheet showing the account reference, support numbers, after-hours availability and the person authorised to request a block. Store a copy somewhere staff can reach without relying on the affected phone system.

At renewal, request the actual contract and service schedule, not only the sales quotation. Check any notification periods, fraud-monitoring exclusions, limits on the provider’s responsibility, charges for urgent support and the process for querying an invoice. If wording is unclear or the potential exposure is material, obtain appropriate advice before signing.

05 When something looks wrong

- Contact your voice provider immediately using a previously verified number. Ask it to investigate and, where appropriate, block the affected extension, destination or outgoing calls.
- Record when the activity was noticed, the extensions or destinations involved and the actions taken. Preserve call records and alerts; avoid deleting potential evidence.
- Have the provider and IT support review portal access, extension credentials, forwarding rules and exposed equipment. Reset affected credentials through a trusted process.
- Check invoices and call records, notify your insurer if relevant, and ask your provider about the dispute and reporting process. Recovery or a credit is not guaranteed.
- Restore services only after the cause and controls have been reviewed, then watch activity closely and document the lessons.

Blocking all outgoing calls can interrupt normal business and emergency calling arrangements. Agree the scope and a safe alternative with the provider as the incident is contained.

Once the immediate problem is contained, reconcile the timeline: when did the unusual calls start, when was the first alert received, who acted and when did the calls stop? Compare the provider’s call records with internal records and keep copies of correspondence. This will help the business understand the remaining exposure and support any discussion with the provider or insurer.

A follow-up should address the cause as well as the bill. If an extension was left active after an employee departed, add phone-system access to the leaving process. If an alert went to an unattended mailbox, change the contact and test delivery. Set a date to confirm that the corrective action was completed.

06 Questions for your provider

- Which destinations are enabled today, and which are excluded from our package?

- Can we block them by extension or time, and who can authorise an exception?
- What alerts and automatic limits are available, how quickly do they operate, and who receives them?
- Who manages credentials, voicemail PINs, forwarding and administrator access?
- What happens after hours, and how do we reach support if our phones are down?
- What does our contract say about disputed or fraudulent call charges?

07 Review the basics together

A phone system is a working business service with settings, access rights and costs that change over time. A short review with the provider can reveal unused extensions, unnecessary destinations and alerts that nobody receives. Record the agreed actions, owners and review date, and revisit them when the business adds a site, changes provider or alters how staff make calls.

Related Energise reports

The customer calls your business. What happens next?

The office devices your cybersecurity policy forgot