APEX ENGLISH
Your voice. Global.

B2 · BUSINESS ENGLISH

UNIT 8 · B8B

Going public

Theme · Tech & Security

Unit 8 · B8B

Going public

Theme: Tech & Security

Learning objectives

- Draft a 3-sentence public statement about an incident that is honest, human and defensible.
- Use reporting verbs (admit, deny, confirm, acknowledge, decline to comment, refute) with the correct grammar.
- Know the difference between what you SAY, what you IMPLY, and what you REFUSE to say — and why the difference matters in crisis comms.

Ask the teacher — notes to bring to class

Class Book

Warm-up · A statement you remember

Think of a public statement from a company AFTER something went wrong — an outage, a breach, a scandal. In 45 seconds out loud: did they land it, or make it worse? Then record a 30-second voice note about the ONE line that stuck with you.

Was it out within HOURS, or DAYS?

Did they say what happened — or hide behind 'unauthorised third-party access'?

Did they say sorry, or 'we regret any inconvenience'?

Bonus: did their share price / user trust survive the statement?

Lead-in: lands or leaks?

Decide: LANDS (honest, specific, human) or LEAKS (hedged, corporate, worse than silence).

1. 'We got this wrong. Your data was exposed for 4 hours. Here is what we're doing.'

---

2. 'We are aware of reports of a potential incident affecting some users.'

---

3. 'A configuration error exposed 12,000 email addresses. No passwords or payment data were affected.'

---

4. 'We take the security of our users extremely seriously.'

---

followUp: Which of the LANDS lines could you steal for your next crisis note?

LANDS

LEAKS

Reading: The three-sentence public statement

Every incident that leaves your building becomes a story. If you don't tell it within hours, someone else will — and they will get it wrong. The default corporate reflex is silence, then hedged language ('we are aware of reports of a potential incident'), then, days later, a legal-sanitised statement that says almost nothing. That timeline is now understood by users as the shape of dishonesty. In 2026, silence and hedge cost more trust than a specific, uncomfortable truth. The best crisis statements are three sentences: what happened, what we know so far, what we're doing about it — sent within hours, updated as facts arrive, and signed by a named human, not 'the team'.

The grammar of the crisis statement is reporting verbs, and each one carries a load. ACKNOWLEDGE = we accept the fact ('we acknowledge that customer email addresses were exposed'). CONFIRM = we've verified the fact ('we can now confirm that no payment data was affected'). ADMIT = we accept a

Ask the teacher — notes to bring to class

fact that is bad for us ('we admit that our internal review missed this vulnerability in April'). DENY = we reject a specific claim ('we deny that any customer credit card data was accessed'). REFUTE = we reject a claim WITH EVIDENCE (this is stronger than deny, and legally different — don't use it unless you have the evidence). DECLINE TO COMMENT = we're saying nothing yet — appropriate for an active investigation, damaging if used to dodge basic facts. Get one of these wrong and the follow-up story writes itself.

The most expensive verb in crisis comms is the one you didn't use. If you didn't SAY it, you didn't IMPLY it — but journalists and users infer aggressively. 'We haven't seen evidence of X' is heard as 'X almost certainly happened, but we're not admitting it yet'. 'We are looking into it' is heard as 'we knew and did nothing'. The professional move is to say what you know, name what you don't know yet, and commit to a specific time when you'll say more ('a full update by 18:00 Lisbon time today'). Silence and vagueness aren't neutral in a crisis — they're a story, and it's always worse than the truth.

1. The best crisis statement is…

   (A) A one-page press release drafted by legal over three days

   (B) Three sentences — what happened, what we know, what we're doing — sent within hours and signed by a named human

   (C) A tweet from an anonymous account

2. 'We can confirm no payment data was affected' uses the reporting verb CONFIRM because…

   (A) It sounds legal

   (B) It means we've verified the fact — stronger than 'we believe'

   (C) It's the same as DENY

3. REFUTE differs from DENY because…

   (A) They're synonyms

   (B) REFUTE means to reject a claim WITH EVIDENCE — legally stronger and only correct if you have the evidence

   (C) REFUTE is informal

4. 'We are aware of reports and looking into it' is dangerous because…

   (A) It's too specific

   (B) In 2026 users read it as 'we knew and did nothing' — vagueness is a story too

   (C) It uses the passive

Vocabulary in context

Match the crisis-comms phrase to its plain-English meaning.

holding statement — the first, short public statement while facts are still being gathered

on the record — quotable, attributable to a named person or the company

off the record — not for publication and not attributable — journalist agreement required

material impact — large enough to matter to investors, users or regulators

Ask the teacher — notes to bring to class

customer notification — the direct email/in-app message to affected users

post-incident update — the follow-up statement once the investigation is more complete

Vocabulary: statements, reporting verbs, and crisis comms

holding statement — the first short statement while facts are being gathered

public statement — the official on-the-record message from the company

customer notification — direct email/in-app to affected users

post-incident update — the fuller follow-up once investigation is further along

attributable quote — a sentence a named individual is willing to have attributed to them

no-comment (v.) — decline to answer a specific question — used sparingly

acknowledge (that) — accept the fact, without necessarily admitting fault

confirm (that) — verify a fact — you've checked

admit (that) — accept a fact that is bad for you

deny (that / -ing) — reject a specific claim

refute (that) — reject a claim WITH evidence — legally stronger than deny

decline to comment (on) — explicitly refuse to answer, on the record

get ahead of the story — pre-empt the narrative before it escapes your control

on / off the record — quotable / not quotable, agreed with the journalist

material impact — large enough to matter to investors, users or regulators

reputational damage — erosion of how the company is perceived

commit to a next update at [time] — name the exact time you'll say more — bounds the silence

single point of contact (SPOC) — one named person handling all press / customer questions

practice

Complete each sentence with ONE word / phrase.

1. We can ___ that no payment data was accessed — the audit finished at 03:00.

2. The CEO ___ that the internal review missed this vulnerability in April — a hard sentence to write, but the right one.

Ask the teacher — notes to bring to class

3. We ___ ___ ___ on the pending regulatory investigation — that's a genuine 'we can't say', not a dodge.

4. Get the ___ ___ out within two hours — we don't need to know everything to say something.

5. Route every press question through one ___ ___ ___ ___ — no comms from anyone else, on any channel.

6. The statement will ___ that we ___ a next update at 18:00 Lisbon time — bounds the silence, buys us four hours.

Practice 2 — collocations & rewrite

Rewrite each sentence replacing the underlined phrase with ONE word/expression from this lesson's vocabulary. Keep the meaning identical.

1. We need to get the <u>first short public message</u> out within the next thirty minutes.

2. The company will <u>accept the fact</u> that email addresses were exposed.

3. We can <u>reject the claim with evidence</u> that passwords were leaked; our logs show no such access.

4. It is vital that we <u>pre-empt the narrative before it escapes</u> our control.

5. The breach is expected to have a <u>large enough effect to matter to investors</u>.

Practice 3 — discursive writing (business memo)

prompt: Draft a crisis communications strategy memo to the Executive Committee regarding a recent data exposure incident.

Use at least FOUR of the target expressions from this unit.

Adopt a professional register: concise, structured, executive-friendly.

Include a clear recommendation or takeaway in the final sentence.

sample: To get ahead of the story, we must issue a holding statement by 10:00 AM today. We should acknowledge the exposure of customer emails while we confirm that no financial data was touched. It is critical that we avoid defensive hedging; instead, we will admit that our internal audit missed the

Ask the teacher — notes to bring to class

vulnerability in the legacy portal. To minimise reputational damage, we have designated the CISO as the single point of contact for all media inquiries. Any claims that passwords were compromised should be handled carefully—we will deny this out loud but only refute it once the forensic logs are fully verified. We commit to a post-incident update for all affected users by end of day. Recommendation: transparency now is the only way to preserve user trust and mitigate the material impact on our upcoming funding round.

Practice B — Weigh the reporting verb

Match each reporting verb to the weight it carries in a public statement.

acknowledge — accept the fact — no fault claim attached

confirm — verify a fact — you have checked and it holds

admit — accept a fact that is BAD for you

deny — reject a specific claim

refute — reject a claim WITH evidence — legally stronger; don't use without proof

decline to comment — explicitly refuse to answer — appropriate for active investigations only

Practice C — Rewrite hedge as a clean line

Each line is corporate hedge. Rewrite it as a LANDS line using ONE reporting verb + the fact.

1. 'We are aware of reports of a potential incident affecting some users.'

2. 'We take the security of our users extremely seriously.'

3. 'We are looking into it and will provide further information in due course.'

4. 'The company refutes any suggestion of wrongdoing.'

Practice D — Odd one out

Which word in each group does NOT belong to the same field?

1. holding statement · customer notification · post-incident update · runbook

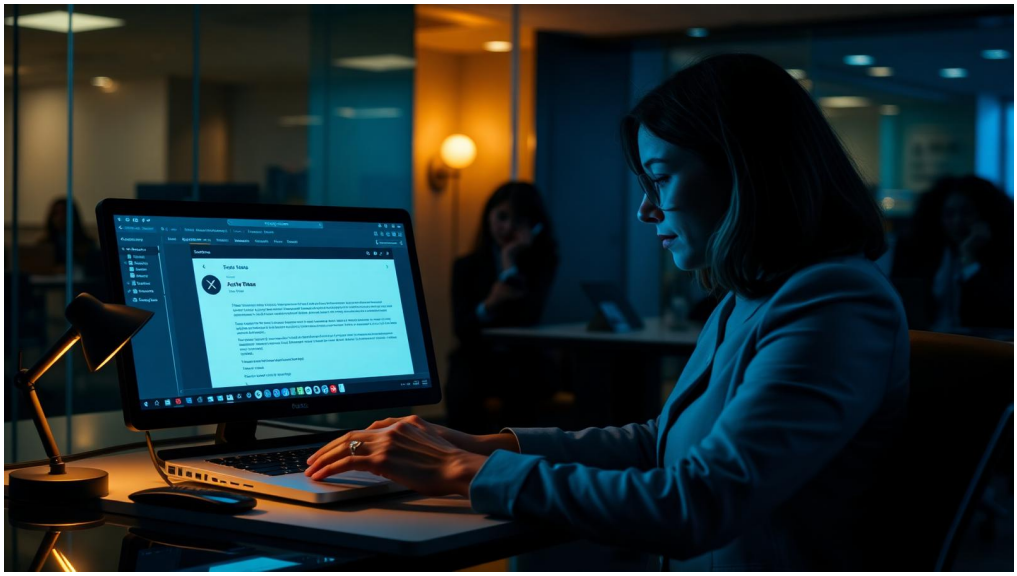
2. acknowledge · confirm · admit · deploy

3. on the record · off the record · attributable quote · blast radius

Ask the teacher — notes to bring to class

4. material impact · reputational damage · SPOC · vulnerability

---



Grammar focus: Reporting verbs

1. ACKNOWLEDGE / CONFIRM / ADMIT — grammar & load — All three take a THAT-clause: 'we acknowledge THAT customer emails were exposed', 'we confirm THAT no payment data was affected', 'we admit THAT our review missed this'. Load: ACKNOWLEDGE = accept the fact, no fault claim. CONFIRM = we've verified the fact. ADMIT = we accept a fact that is BAD for us. ADMIT can also take -ING for actions: 'the company admitted DELAYING notification by 36 hours' — grammatical, but heavier than 'admitted that notification was delayed'.

2. DENY / REFUTE / REJECT — the negative side — DENY + that-clause: 'we deny THAT any credit card data was accessed'. DENY + -ing: 'we deny KNOWING about the vulnerability before Tuesday'. REFUTE = deny WITH evidence — 'we refute the claim that customer data was sold; our access logs show no external export'. Do NOT use 'refute' as a fancy synonym for 'deny' — journalists notice, and if you can't produce the evidence, you look worse than if you'd just said 'deny'. REJECT = stronger than deny for a claim or accusation — 'we reject the characterisation that our team was warned in April'.

3. DECLINE TO COMMENT / DECLINE TO CONFIRM / DECLINE TO ELABORATE — Form: DECLINE + TO + infinitive. 'The company DECLINED TO COMMENT on the pending investigation.' 'The CEO DECLINED TO CONFIRM the exact number of affected users.' Appropriate when: active regulatory investigation, criminal case, personnel matter, or specific number not yet verified. Dangerous when: used to dodge a fact you clearly know. 'No comment' on 'was our data exposed?' reads to users and journalists as 'yes, and we're hoping you'll go away'.

Ask the teacher — notes to bring to class

4. Common traps — • 'We denied the incident' ✗ (ambiguous) → 'we denied THAT any customer data was accessed' (specific claim). • 'We refute your allegations' — if you have no evidence, this is a lie. Use 'deny' instead. • 'Admits to X' ≠ 'admits X'. 'The company admits TO delaying' is spoken English but rarer in written statements — prefer 'admits that…' or 'admits delaying'. • 'We are not aware of any…' — sounds like ignorance is a defence. It isn't. If you're not aware, say when you'll find out ('we will confirm one way or the other by 18:00').

Exercise A — Choose the right reporting verb

Complete each sentence with ONE of: acknowledge / confirm / admit / deny / refute / decline to comment.

1. We can ___ that no payment data was accessed — the audit finished at 03:00.

2. The CEO ___ that our internal review missed this vulnerability in April.

3. The company ___ ___ ___ on the pending regulatory investigation.

4. We ___ any suggestion that this data was sold — our access logs show no external export. (STRONG — with evidence)

5. We ___ that customer email addresses were exposed for approximately 4 hours yesterday.

6. The spokesperson ___ that any credit card data had been accessed.

Exercise B — Rewrite the hedge as a statement

Rewrite each dodgy corporate line as a specific, honest reporting-verb sentence.

1. 'We are aware of reports of a potential incident affecting some users.'

2. 'We are looking into these matters and will provide an update in due course.'

3. 'We take the security of our users extremely seriously.'

4. 'We refute all allegations made in the press.'

Ask the teacher — notes to bring to class

Exercise C — Draft the holding statement (3 sentences)

The facts: at 14:02 yesterday, a configuration error exposed approximately 12,000 customer email addresses for 3 hours 54 minutes. No passwords or payment data were involved. You will notify each affected user by email within 24 hours. Draft the 3-sentence holding statement. It MUST include: (1) ONE 'acknowledge' or 'confirm', (2) explicit boundary of the impact ('no ___ was affected'), (3) a named next commitment with a specific time.

1. Draft the statement.

Listening: three CEO statements about the same breach

You're a customer of Novavault, a Portuguese fintech. Yesterday evening they suffered a data breach exposing customer email addresses. This morning three drafts of the CEO's public statement leaked to a tech reporter — from three different comms teams. You're listening to which one lands. You're not a comms professional; you're a customer trying to decide whether to keep your money with them.

pre

Which speaker do you predict will land it — and what will make you keep your money there?

Think of a company that DID lose your trust after a breach. What was the sentence that lost it?

gist

1. Which CEO's statement earns back trust, and why?

2. Which statement makes the story worse than the actual breach?

3. Which statement is technically fine and still fails?

detail

1. What are the EXACT three claims in Sofia's opening — and what reporting verb sits under each?

2. What SPECIFIC time-bounded commitment does Sofia make, and why does it matter?

Ask the teacher — notes to bring to class

3. What is the ONE line in Beatriz's over-legal statement that is technically correct but does the most damage?

Third listen — comms craft

Focus on HOW each CEO uses language and structure. Answer from what they DO.

1. Sofia includes a hard admission ('we should have detected this faster'). Isn't that a legal risk?

2. Diogo's statement is 'safe' in the sense that it says nothing. Why is that the least safe move?

3. Beatriz's draft is passive, un-signed, and 'in due course'. What single word would save it?

Language from the audio — crisis-comms moves worth stealing

Match each phrase to what it DOES.

"We acknowledge that ~12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday." — acknowledge + specific number + specific window = fact, not hedge

"We can confirm that no passwords, payment information or account balances were accessed." — confirm + explicit BOUNDARY of impact = reassurance where it's warranted

"We should have detected this faster." — specific, bounded admission = closes the story down; hedge invites speculation

"Every affected user will receive a direct email by 12:00 tomorrow; full post-incident report within 14 days." — TWO named times = bounds the silence at both ends, proves urgency and thoroughness

"We are aware of reports of a potential incident affecting some users." — hedged silence = invites others to define the story, expands liability

"The affected parties will be contacted in due course." — passive + no time + 'parties' = technically correct, emotionally absent, damaging

Voice A (Diogo — hedging draft): We are aware of reports of a potential incident affecting some of our users yesterday afternoon. We take the security of our users extremely seriously. Our team is actively looking into these matters, and we will provide a further update in due course. — The Novavault team.

Ask the teacher — notes to bring to class

Voice B (Sofia — the CEO): We acknowledge that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday, as a result of a configuration error which has now been fixed. We can confirm that no passwords, payment information or account balances were accessed. And I want to be direct about one thing: we should have detected this faster — the alert that would have caught it had been misconfigured, and we are addressing that this week. Every affected user will receive a direct email notification by 12:00 tomorrow. A full post-incident report will be published within 14 days, and I will personally answer questions on it live. — Sofia Duarte, CEO.

Voice C (Beatriz — over-legal draft): It has been determined that a data exposure incident occurred on the platform yesterday. Appropriate steps are being taken to investigate the circumstances and remediate any weaknesses identified. The affected parties will be contacted in due course. Any further inquiries should be directed to press@novavault.pt. — Signed, the Communications Office.

Speaking: solo role-play — 90-second crisis briefing

Solo task. Pick ONE incident YOUR company (or a company you know) faced in the last two years — outage, breach, product recall, staffing scandal. Record yourself (voice note, up to 90 seconds) delivering the CEO's public statement out loud. You MUST include: (1) ONE 'acknowledge' or 'confirm' + a SPECIFIC number and time window, (2) ONE 'we can confirm that no ___ was affected' — the boundary line, (3) ONE 'admit' — the uncomfortable operational truth, (4) TWO named time commitments — the short (24h) one and the long (14-day) one, (5) sign it with a name — real or made-up.

Scene: A real recent incident at your company / industry (recommended)

A: You deliver the CEO statement.

B: Imagined listener: your customers, reading it on your website within 4 hours of the incident.

Scene: A hypothetical: your product exposed customer emails for 4 hours

A: You deliver the CEO statement.

B: Imagined listener: a tech reporter, who will publish quotes.

Scene: A staffing / safety scandal at a company you follow

A: You deliver the imagined CEO statement.

B: Imagined listener: employees, who will forward it to journalists if it feels false.

Extra speaking task — 30-second 'the sentence that closes the story'

Compress the whole statement to ONE sentence — the sentence a journalist would quote if they only had one line. Record a 30-second voice note. Format: 'We [acknowledge / confirm] that [specific fact + specific window]; we can confirm no [X] was affected; we should have [uncomfortable truth]; next update at [specific time]. — [Name].'

Ask the teacher — notes to bring to class

Writing mini-task

Draft the 3-sentence holding statement (max 80 words) for a hypothetical incident at YOUR company. It MUST include: (1) ACKNOWLEDGE or CONFIRM + a specific number and time window, (2) the boundary — 'we can confirm no ___ was affected', (3) ONE named commitment with a specific time. Sign it with a real name and a real role — not 'the team'.

Wrap-up

One reporting verb from today (acknowledge / confirm / admit / deny / refute) you'll use precisely, not casually.

One 'we take X seriously' sentence you'll DELETE from any future statement — and what you'll replace it with.

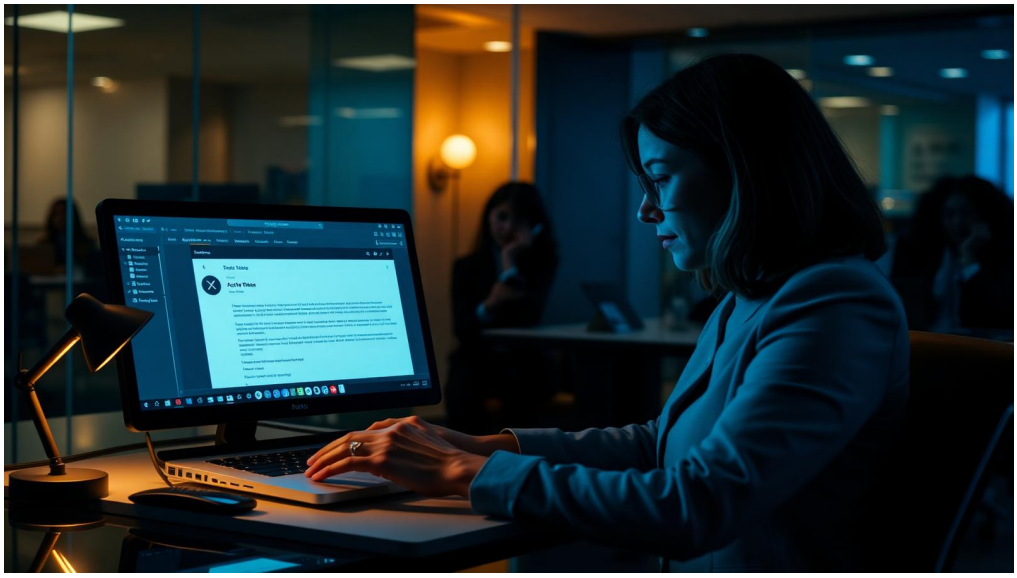
One time-boxed commitment format ('by 12:00 tomorrow / within 14 days') you'll steal for your next crisis note.

Quiz

1. The best crisis statement is…
   (A) A one-page release drafted by legal over three days
   (B) Three sentences within hours, signed by a named human, updated as facts arrive
   (C) A single tweet
2. REFUTE is stronger than DENY because…
   (A) It's more polite
   (B) REFUTE means to reject a claim WITH EVIDENCE — only use it if you have the evidence
   (C) It's less formal
3. 'We are aware of reports of a potential incident' is dangerous because…
   (A) It's a passive voice error
   (B) In 2026 users read hedged silence as 'we knew and did nothing'
   (C) It's too specific
4. 'We take the security of our users extremely seriously' should be…
   (A) Kept — it's reassuring
   (B) Deleted — every company writes it and it says nothing; replace with what you're DOING
   (C) Repeated three times
5. The best statement includes TWO time commitments — a short one and a long one — because…
   (A) Longer sounds more official
   (B) The short one proves urgency; the long one bounds the silence and proves the investigation isn't rushed
   (C) Legal requires two

Ask the teacher — notes to bring to class

Workbook — home practice



Exercise 1 — Crisis-comms vocabulary

Complete each sentence with ONE phrase from the box.

Word bank: holding statement · single point of contact · material impact · customer notification · post-incident update · off the record

1. Issue the ___ ___ within two hours — we don't need every fact confirmed to say something.

2. Route every press question through one ___ ___ ___ ___ — no comms from anyone else.

3. The breach exposed 47,000 records — that constitutes a ___ ___, and the regulator has to be notified.

4. Every affected user will receive a direct ___ ___ by 12:00 tomorrow.

5. The full ___-___ ___ will be published within 14 days.

6. She'd speak to us ___ ___ ___, but not on the record.

Ask the teacher — notes to bring to class

Exercise 1b — Vocabulary — discursive writing

Write a crisis communication strategy (120–180 words) for the Executive Board following a security breach. Outline how to handle public and internal messaging. Incorporate at least four phrases from Exercise 1: holding statement, single point of contact, material impact, customer notification, post-incident update, or off the record.

type: writing

Use at least 4 target vocabulary items from the unit.

Maintain a formal, high-stakes crisis register.

Use strong reporting verbs (e.g., 'confirm', 'refute', 'acknowledge').

Structure clearly: Immediate Actions, Communication Channels, Long-term Plan.

model: Subject: Crisis Communication Strategy — Data Exposure To the Executive Board, In light of the recent data exposure, our primary objective is to maintain market trust through transparency. We have already issued an initial holding statement to acknowledge the incident, and Sofia has been designated as the single point of contact for all media inquiries to ensure a unified voice. While the incident had no material impact on financial data, the exposure of customer names requires a rigorous customer notification process, which will be completed by 18:00 today. We must avoid giving any off the record comments to reporters, as these can lead to damaging speculation. Instead, we will focus on providing a comprehensive post-incident update once the full forensic audit is concluded in 14 days. Our reputation depends on our ability to demonstrate competence and accountability during this window.

Exercise 2 — Reporting verbs

Complete each sentence with ONE of: acknowledge / confirm / admit / deny / refute / decline to comment.

1. We can ___ that no payment data was accessed — the audit finished at 03:00.

2. The CEO ___ that our internal review missed this vulnerability in April.

3. The company ___ ___ ___ on the pending regulatory investigation.

4. We ___ any suggestion that the data was sold — our logs show no external export. (STRONG — with evidence)

5. We ___ that ~12,000 customer email addresses were exposed yesterday.

6. The spokesperson ___ that any credit card data had been accessed.

Ask the teacher — notes to bring to class

Exercise 3 — Lands or leaks?

Decide whether each statement LANDS (honest, specific, human) or LEAKS (hedged, corporate, worse than silence).

1. 'We got this wrong. Your data was exposed for 4 hours. Here is what we're doing.'
   (A) LANDS
   (B) LEAKS
2. 'We are aware of reports of a potential incident affecting some users.'
   (A) LANDS
   (B) LEAKS
3. 'A configuration error exposed 12,000 email addresses. No passwords or payment data were affected.'
   (A) LANDS
   (B) LEAKS
4. 'We take the security of our users extremely seriously.'
   (A) LANDS
   (B) LEAKS
5. 'The affected parties will be contacted in due course.'
   (A) LANDS
   (B) LEAKS
6. 'Every affected user will receive a direct email by 12:00 tomorrow.'
   (A) LANDS
   (B) LEAKS

Exercise 4 — Rewrite the hedge as a statement

Rewrite each dodgy corporate line as a specific, honest reporting-verb sentence.

1. 'We are aware of reports of a potential incident affecting some users.'

2. 'We are looking into these matters and will provide an update in due course.'

3. 'We take the security of our users extremely seriously.'

4. 'We refute all allegations made in the press.'

Ask the teacher — notes to bring to class

Exercise 5 — Three CEO statements about the same breach

You'll hear three drafts of the same public statement from Novavault. Decide which one earns back trust, which makes the story worse, and which is technically fine but still fails.

1. Which statement earns back trust?

2. Which statement makes the story worse than the breach?

3. Which statement is technically fine and still fails?

Voice A (Diogo — hedging draft): We are aware of reports of a potential incident affecting some of our users yesterday afternoon. We take the security of our users extremely seriously. Our team is actively looking into these matters, and we will provide a further update in due course. — The Novavault team.

Voice B (Sofia — the CEO): We acknowledge that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday, as a result of a configuration error which has now been fixed. We can confirm that no passwords, payment information or account balances were accessed. I want to be direct: we should have detected this faster — the alert that would have caught it had been misconfigured, and we are addressing that this week. Every affected user will receive a direct email by 12:00 tomorrow. A full post-incident report will be published within 14 days. — Sofia Duarte, CEO.

Voice C (Beatriz — over-legal draft): It has been determined that a data exposure incident occurred on the platform yesterday. Appropriate steps are being taken to investigate the circumstances and remediate any weaknesses identified. The affected parties will be contacted in due course. Any further inquiries should be directed to press@novavault.pt. — Signed, the Communications Office.

Exercise 6 — Draft the 3-sentence holding statement

Facts: at 14:02 yesterday, a configuration error at YOUR company exposed 12,000 customer email addresses for 3h 54min. No passwords or payment data involved. You will notify affected users within 24h. Draft the 3-sentence holding statement (max 80 words). Include: (1) ACKNOWLEDGE or CONFIRM + specific number and window, (2) explicit boundary ('no ___ was affected'), (3) ONE named next commitment with a specific time. Sign it with a real name and role.

Exercise 7 — Case study reflection: Novavault

Think about the Novavault case (47,000 customers, email+name+truncated IBAN exposed for ~4h, reporter deadline at 12:00, false '500k' claim spreading). Answer the questions.

Ask the teacher — notes to bring to class

1. Sequence your first four hours (09:00–13:00). What do you publish and in what order — and why that order?

2. The anonymous X account is claiming '500k records'. Do you engage? What do you post?

3. Legal wants you to soften 'we should have detected this faster' to 'we are reviewing our detection processes'. What do you say?

Ask the teacher — notes to bring to class

Answer key — Class Book

Lead-in: lands or leaks?

1. LANDS — owns it, specific window, action next.
2. LEAKS — 'aware of reports' says nothing, 'potential' is denial.
3. LANDS — the number, the boundary, the reassurance.
4. LEAKS — the sentence every company writes when they have nothing to say.

Reading: The three-sentence public statement

1. (B) Three sentences — what happened, what we know, what we're doing — sent within hours and signed by a named human
2. (B) It means we've verified the fact — stronger than 'we believe'
3. (B) REFUTE means to reject a claim WITH EVIDENCE — legally stronger and only correct if you have the evidence
4. (B) In 2026 users read it as 'we knew and did nothing' — vagueness is a story too

Vocabulary: statements, reporting verbs, and crisis comms

1. confirm
2. admitted
3. decline to comment
4. holding statement
5. single point of contact
6. commit / to

1. We need to get the holding statement out within the next thirty minutes.
2. The company will acknowledge that email addresses were exposed.
3. We can refute the claim that passwords were leaked; our logs show no such access.
4. It is vital that we get ahead of the story.
5. The breach is expected to have a material impact.

1. Model: 'We can CONFIRM that a data-exposure incident affected approximately 12,000 users between 09:00 and 13:00 today.'
2. Model: 'We ACKNOWLEDGE that customer email addresses were exposed. Full customer notifications go out today by 18:00.'
3. Model: 'We are investigating and COMMIT TO a full public update by 18:00 Lisbon time today, signed by the CISO.'
4. Model: 'We DENY that any credit card data was accessed; our access logs show no external export in the affected window.' (Only use 'refute' if you can produce the evidence.)

1. runbook — the other three are public/customer-facing artefacts; a runbook is internal.
2. deploy — the other three are reporting verbs; deploy is an engineering action.
3. blast radius — the other three are press-handling terms; blast radius belongs to incident scoping.
4. vulnerability — the other three describe crisis stakes and roles; vulnerability is a security term.

Grammar focus: Reporting verbs

1. confirm
2. admitted
3. declined to comment
4. refute
5. acknowledge
6. denied

1. Model: 'We ACKNOWLEDGE that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday. We CONFIRM that no passwords or payment data were affected. A full update will be published by 18:00 today.'
2. Model: 'We are actively investigating and will publish a specific update by 18:00 Lisbon time today. In the meantime we can CONFIRM that the affected service was restored at 17:56 and that no payment data was involved.'

Ask the teacher — notes to bring to class

3. Model: (delete it — say what you're actually DOING.) 'We have engaged an external forensics firm; we will notify every affected user directly by 12:00 tomorrow; we will publish the post-incident review within 14 days.'
4. Model: (only if you have the evidence.) 'We REFUTE the claim that customer data was sold to a third party — our access logs, which we have shared with the regulator, show no external export.' If you can't share the evidence, DOWNGRADE to: 'We DENY that any customer data was sold.'
1. Model: 'We ACKNOWLEDGE that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday due to a configuration error, which has now been fixed. We CONFIRM that no passwords, payment information or personal data beyond email addresses were affected. Every affected user will receive a direct notification by email within the next 24 hours, and a full post-incident report will be published within 14 days — signed, [CEO name].'

Listening: three CEO statements about the same breach

1. Voice B (Sofia, real CEO). Names the fact, names the boundary, names the action, names the next update time. Uses ACKNOWLEDGE and CONFIRM correctly, uses ADMIT for the uncomfortable bit ('we should have detected this faster'), signs it with her own name. Sounds like a human.
2. Voice A (Diogo, hedging draft). 'We are aware of reports of a potential incident.' 'We are looking into it.' 'We take security extremely seriously.' Every sentence a hedge, no numbers, no time commitment, signed 'the Novavault team'. Users read it as 'we knew, we're stalling, we hope you go away'.
3. Voice C (Beatriz, over-legal draft). Facts are correct, verbs are correct — but the whole statement is passive, un-signed, and reads as if written for regulators, not humans. 'It has been determined that…' 'Steps are being taken…' 'The affected parties will be contacted in due course.' Technically correct, emotionally absent — customers can smell it.
1. 1. ACKNOWLEDGE — 'we acknowledge that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday.' 2. CONFIRM — 'we can confirm that no passwords, payment information or account balances were accessed.' 3. ADMIT — 'we should have detected this faster — the alert that would have caught it had been misconfigured, and we're addressing that this week.' Fact, boundary, hard truth — in that order, in her own voice.
2. 'We will publish a full post-incident report within 14 days, and every affected user will receive a direct email by 12:00 tomorrow.' Two named times: 12:00 tomorrow (short — proves urgency, forces her own team to move), and 14 days (long — proves the full investigation isn't rushed). Bounds the silence at both ends. Diogo makes no time commitment; Beatriz says 'in due course' — which reads as 'never'.
3. 'The affected parties will be contacted in due course.' PASSIVE (who?), no time, and 'affected parties' turns customers into 'parties' — a legal category, not a human. Customers reading their own breach notice want their status ('you were affected'), the specific data ('your email address'), and a specific action ('by tomorrow noon'). Beatriz gives none of the three.
1. The received wisdom says yes; the evidence says no. A specific, bounded admission ('we should have detected this faster; the alert had been misconfigured; we're addressing it this week') closes the story down. A hedge invites weeks of speculation — during which every leaked detail expands liability. The bigger legal risk in 2026 is a statement that is later shown to have known-false hedges in it, not one that admits an operational failure and commits to fixing it.
2. Because the story fills the vacuum. Reporters, regulators, users, and competitors all fill Diogo's silence with their own worst-case theory — and by day three, Novavault is defending accusations that are worse than the actual breach. 'We are aware of reports' is not neutral; it's an active invitation for others to define the story. Silence is a statement, and it always says the wrong thing.
3. A name. Signing it 'Sofia Duarte, CEO' converts an anonymous corporate emission into a human accountability. It also changes the writer's own behaviour — you write differently when your name is on it. 'Signed by the Novavault team' is the modern equivalent of 'no one is responsible'. In a crisis, one named human is worth ten pages of legal-safe passive.

Quiz

1. (B) Three sentences within hours, signed by a named human, updated as facts arrive
2. (B) REFUTE means to reject a claim WITH EVIDENCE — only use it if you have the evidence
3. (B) In 2026 users read hedged silence as 'we knew and did nothing'
4. (B) Deleted — every company writes it and it says nothing; replace with what you're DOING
5. (B) The short one proves urgency; the long one bounds the silence and proves the investigation isn't rushed

Ask the teacher — notes to bring to class

Answer key — Workbook

Exercise 1 — Crisis-comms vocabulary

1. holding statement
2. single point of contact
3. material impact
4. customer notification
5. post-incident update
6. off the record

Exercise 2 — Reporting verbs

1. confirm
2. admitted
3. declined to comment
4. refute
5. acknowledge
6. denied

Exercise 3 — Lands or leaks?

1. (A) LANDS
2. (B) LEAKS
3. (A) LANDS
4. (B) LEAKS
5. (B) LEAKS
6. (A) LANDS

Exercise 4 — Rewrite the hedge as a statement

1. Model: 'We ACKNOWLEDGE that approximately 12,000 customer email addresses were exposed between 14:02 and 17:56 CET yesterday. We CONFIRM that no passwords or payment data were affected. A full update will be published by 18:00 today.'
2. Model: 'We are investigating and will publish a specific update by 18:00 Lisbon time today. In the meantime we can CONFIRM the affected service was restored at 17:56 and no payment data was involved.'
3. Model: (delete it — say what you're DOING.) 'We have engaged an external forensics firm; we will notify every affected user directly by 12:00 tomorrow; we will publish the post-incident review within 14 days.'
4. Model: (only if you have the evidence.) 'We REFUTE the claim that customer data was sold — our access logs, shared with the regulator, show no external export.' Without evidence, downgrade to DENY.

Exercise 5 — Three CEO statements about the same breach

1. Voice B (Sofia, real CEO) — acknowledges + specific number + specific window; confirms the boundary; admits the operational truth; two named time commitments (12:00 tomorrow + 14 days); signed with her name.
2. Voice A (Diogo — hedging) — 'we are aware of reports of a potential incident', 'we take security extremely seriously', signed 'the Novavault team'. Every sentence a hedge, no numbers, no time commitment.
3. Voice C (Beatriz — over-legal) — passive, un-signed, 'in due course'. Facts are right, verbs are right, but reads as if written for regulators, not humans.

Exercise 7 — Case study reflection: Novavault

1. Model: 09:30 alignment call (CEO/CISO/legal/comms). 10:00 draft in CEO inbox. 10:30 Sofia records 60-sec video. 11:00 publish written statement + video on site. 11:15 email affected customers directly. 11:30 reply to Observador reporter with the full statement. Result: at 12:00 the story lands with OUR numbers and OUR voice, not the reporter's.
2. Model: Do NOT engage the account directly (feeds algorithm, legitimises a 900-follower voice). DO publish a calm correction on our own channel: '~47,000 customers were affected. Some social reports suggest higher numbers; these are inaccurate. If you have not received an email by 18:00 CET, your account was not affected.' The correction carries a piece of useful information, not just a fight.

Ask the teacher — notes to bring to class

3. Model: The specific admission closes the story down within 48h. The hedge invites weeks of speculation — during which every leaked internal detail expands liability. Regulators and users in 2026 read the hedge as evasion; they read the admission as competence. Land the point; if legal insists, negotiate to 'we should have detected this faster; the alert responsible had been misconfigured, and that has been corrected'.

Ask the teacher — notes to bring to class