



PRIVATE SECTOR SECURITY SERIES

Insider Risk and Social Engineering Defense

A practical handbook for private companies

JOSHUA D. TATRO / EXPANDED LEARNING EDITION



FOREWORD

Security begins with judgment

A note from Joshua D. Tatro

Private companies depend on people being able to trust one another. Employees need access to do their jobs; vendors and partners need enough information to help. Security has to work within those relationships.

I have spent most of my professional life in environments where trust and security have to coexist. The lesson I keep coming back to is that effective security is rarely about catching a person in a single moment. It is about seeing the whole picture early enough to prevent harm.

Deliberate theft and sabotage belong in that picture. So do a well-meaning employee who bypasses a safeguard to meet a deadline, a technician manipulated by a convincing caller, and a vendor whose access quietly grows beyond its purpose.

This handbook gives employees and leaders a practical way to recognize those situations. It explains what to notice, when to verify, and how to report a concern without guessing at someone's motives.

There is no reliable checklist that tells you who can be "bought." Personal hardship or dissatisfaction is not evidence of disloyalty. An offer of payment for nonpublic information, an attempt to conceal access, or a repeated request to bypass a control is something concrete that a company can assess.

Our aim is better decisions under pressure. Employees should be able to ask for help without fear of being blamed. Leaders should respond proportionately, preserve privacy, and correct the conditions that made an unsafe shortcut attractive.

This expanded edition adds practical teaching, two documented IP cases, and exercises with debriefs. Use them to practice reasoning before a real concern puts the team under pressure.

Joshua D. Tatro

Chief Operating Officer
Copperhead Consulting Inc

**A learning handbook for private companies**

Recognize meaningful conduct. Protect valuable information. Make a defensible decision.

LEARNING MAP

How to learn from this handbook

Read, apply, discuss, and then improve the process.

This handbook teaches employees, managers, and security teams how to reason about insider risk. By the end, you should be able to describe a useful indicator, distinguish an account from its user, evaluate a request for sensitive access, and report facts without declaring someone guilty.

The reading route

Pages 4-10: understand insider risk, evaluate observations, recognize manipulation, and interpret workplace and technical signals. Start here if the subject is new to you.

Pages 11-15: identify intellectual property, map physical and third-party access, and connect controls to business consequences. Managers, Procurement, IT, and project owners should work through these pages together.

Pages 16-20: practice intake, proportionate response, evidence handling, and management conversations. These pages explain where ordinary reporting ends and an authorized assessment begins.

Pages 21-24: study two documented cases and their separate debriefs. One concerns employee theft; the other concerns a commercial partner obtaining IP through an insider. Facts and CCI recommendations are distinguished.

Pages 25-27: run two fictional tabletop exercises and compare your decisions with the debrief. **Pages 28-32:** build a program, use the field tools, clarify terms, and consult sources.

Use it with a team

Read one topic before a short discussion. Ask participants to identify a fact, a plausible alternative explanation, and the next authorized action. Finish by assigning an improvement to a named owner. The exercises test the process, not an employee's character.

References [1-5] support the general framework. CCI's examples, questions, and workflows are educational recommendations, not validated predictors of misconduct. Use local policy, emergency contacts, and qualified advice when implementing them.



THE OPERATING PICTURE

Understanding insider risk

Authorized access can be misused, stolen, or manipulated.

An insider is anyone whose access, knowledge, or proximity could affect the organization. Employees and executives are part of that group, but so are contractors, vendors, temporary staff, and former personnel whose access remains active.

Four ways harm can happen

Malicious misuse is deliberate abuse of trust: theft, fraud, sabotage, disclosure, or violence. **Negligent conduct** bypasses a safeguard and can expose data or systems even without an intention to cause harm.

Compromise means an outsider controls an account, device, or trusted relationship.

Unwitting assistance occurs when someone is deceived into releasing information, resetting credentials, opening a file, or allowing entry. These paths can overlap.

A valid login does not establish who is using it. Equally, an unusual action does not establish malicious intent. A sound assessment checks the work requirement, authorization, timing, and explanation before deciding what to do.

Build a protective cycle

Start with the people, assets, and dependencies whose loss would matter most. Reduce unnecessary access and make approved processes usable. Teach employees to recognize a meaningful change or request, then give them a clear route to report it.

Assign responsibility for verification, assessment, containment, and communication before an incident. After a concern or near miss, review the decision and repair the process. If the explanation is legitimate, record it and close the matter appropriately.

The model on this page is a prompt for questions, not a scoring system. Concern deserves attention when conduct connects to a real opportunity for harm and supporting facts can be checked.



What happened?

What could be affected?

What else supports it?

SOUND JUDGMENT

Read conduct, not character

An indicator is a reason to clarify—not a verdict.

Good reporting describes an action someone else could verify. “She is suspiciously private” tells a reviewer very little. “She refused the required identity check and asked three employees for an exception” identifies a behavior and a control.

The distinction matters when the subject is sensitive. Financial difficulty does not make a person corrupt. An unknown person offering payment for restricted information is a reportable approach. Job dissatisfaction is not sabotage; moving unrelated project files to a personal account is an action that warrants checking.

Keep the evidence separate

Record what you directly observed, what another person alleged, and what you inferred. Include exact words when a threat is made. “He said they would regret blocking him and struck the desk” is more useful than a diagnosis or a label.

Seek corroboration through authorized records or witnesses, but do not postpone an urgent safety report while trying to prove it. A single serious event can require immediate action.

Protect a fair process

Do not treat race, nationality, religion, gender, disability, age, family status, political belief, or lawful off-duty activity as threat indicators. Do not diagnose mental illness. Stress and mental health conditions do not establish dangerousness.

Apply the same review standard to a senior executive and a new hire. Limit information to those with a legitimate role in the response. Financial pressure, travel, a grievance, or a workplace complaint may explain context; none proves harmful intent.

A safe outcome may be a corrected permission, clearer supervision, workload support, an employee assistance referral, or a better process. An investigation is not the inevitable result of every concern.

01

Observable

An action or exact words.

02

Relevant

A connection to work, access, or safety.

03

Corroborated

Supporting records or witnesses. Do not delay an emergency report.

REASONING UNDER UNCERTAINTY

How to interpret a warning sign

A useful assessment tests more than one explanation.

Suppose an employee downloads hundreds of files late on a Friday. The observation is real, but its meaning is not yet established. An approved migration, a time-zone difference, account compromise, and deliberate removal could produce similar records. The next question should distinguish those explanations.

Separate the layers

Write the fact first: which account, which files, which destination, and what time. Then record what is unknown. “The account exported 340 files” does not mean the named employee personally exported them. “No approval was found in the ticket system” is more precise than “There was no approval.”

Compare the activity with the role and the task. Check the relevant period rather than searching indefinitely for a pattern. Ask whether the destination, file sensitivity, or requested privilege changes the consequence. Two records created by the same automated event are not independent corroboration.

Work against confirmation bias

Once a person is suspected, harmless details can begin to look incriminating. Assign someone to identify a plausible innocent explanation and the evidence that would support it. Record information that weakens the concern as carefully as information that strengthens it.

An unusual event can be important without being malicious. In a workplace where serious insider incidents are uncommon, a noisy detector can generate many innocent cases. That is why review quality, false-positive handling, and timely closure matter alongside detection.

Decide despite uncertainty

You do not need certainty to take a reversible protective step when loss is continuing. Temporarily pausing an export is different from accusing an employee. Document the reason, authority, owner, and review time. Immediate danger overrides a leisurely fact-finding process.

Practice question: what single record would most help distinguish a legitimate migration from an unauthorized export? A matching approved task and approved destination would be a strong starting point; neither alone resolves every possibility.

**OBSERVATION**

What the record establishes

ALTERNATIVES

What else could explain it

DECISION

What protection is justified

THE HUMAN ATTACK SURFACE

The request that bends the rules

Social engineering turns a plausible story into an unsafe exception.



CONCEPTUAL EDITORIAL ILLUSTRATION

An attacker may know the project name, the manager, and the deadline. Those details make a story credible; they do not establish identity or authorization. The decisive question is what the person wants you to do.

Notice the pressure

Authority and urgency often arrive together: a supposed executive needs a transfer, or a caller says a launch will fail unless access is restored. Secrecy discourages checking. Fear pushes the recipient toward a link or an unexpected approval. Familiarity, helpfulness, and a previous favor can make refusal feel impolite.

The request may begin harmlessly. A conversation establishes familiarity, then shifts toward a file, a code, a new communication channel, or an exception to the normal process. Later requests may be framed as routine because the first one succeeded.

Verify at the boundary

Pause when the request crosses a control. Use an independently obtained number, the official support portal, a known directory, or an established ticket. Do not verify by calling the number supplied in the suspicious message.

An urgent business need should use the approved emergency process. A confidential request still needs authorization. Access is a business decision, not repayment for a favor.

Voice, video, and email can be imitated. Recognizing a face or voice is weaker than checking through a separate trusted channel. If you have already shared credentials, approved a prompt, or transferred information, report that fact immediately so responders can limit harm.

HUMAN INFLUENCE

Recruitment and coercion

Recognize the approach and the requested action.

The useful question is not whether someone “looks susceptible.” It is whether an outside relationship is pressing them to misuse access. A person may be approached because of a role, a project, or information they can reach. A confident, successful employee can be targeted as readily as someone under financial pressure.

How a boundary changes

A professional conversation may become a paid consultation, then a request for nonpublic details. A gift may be tied to a favor. A contact may ask that a discussion move off approved channels or insist that the company must not know. Each action should be assessed in context; outside work and ordinary networking are not inherently suspicious.

The clearest warning is the request: provide restricted information, share credentials, bypass a review, falsify a record, or conceal a relationship that policy requires the employee to disclose. Increasing payment does not make an unauthorized disclosure legitimate.

When the pressure becomes coercive

Someone may threaten exposure, harm, or professional consequences. An employee who reports that pressure needs a safe route to Security and the appropriate support team. Do not make continued contact, amateur evidence collection, or private negotiation a condition of receiving help.

Employees should preserve existing communications through approved means, stop unauthorized disclosures, and report the requested action and any immediate threat. They should not bargain with the contact or attempt a sting. Security and Legal determine appropriate coordination with authorities.

Make early disclosure workable

Publish a route for reporting gifts, conflicts, suspicious consulting offers, and coercive approaches. Explain who receives the report and the limits of confidentiality. Thank people for reporting promptly, including when they made an initial mistake. Accountability can coexist with support; silence makes containment harder.

Teaching point: being approached is evidence of targeting, not evidence of cooperation. The response should protect the employee while establishing what happened.



WHAT EMPLOYEES MAY NOTICE

When small exceptions add up

Look for actions connected to access, concealment, or harm.

Boundary testing and concealment

Repeated bypass requests, credential sharing, and attempts to find a more permissive approver deserve attention. So do false records, hidden storage, unexplained deletion, or instructions to omit facts. Preserve what you observed; do not search personal property or confront the person.

Collection and preparation

Unusual interest in restricted projects, personnel, schedules, or security routines may need a work-purpose check. Testing controls, staging files, rehearsing explanations, or seeking unauthorized methods becomes more concerning when linked to sensitive access.

External pressure

An offer of payment, a concealed gift tied to access, blackmail, or coercion is a reason to seek help. Make it safe to report an approach before anyone complies. The fact that a person was targeted does not mean they cooperated.

Grievance and threats

Record fixation on retaliation, named targets, intimidation, stalking, or statements suggesting attack planning in the person's exact words. Use workplace-violence procedures. For imminent harm, move to safety and contact emergency services; do not wait to collect a pattern.

Changes around departure

Bulk collection, personal repositories, retained credentials, and new forwarding routes should be checked against approved work. Use consistent offboarding standards rather than treating every departing employee as a suspect.

Patterns that are easy to miss

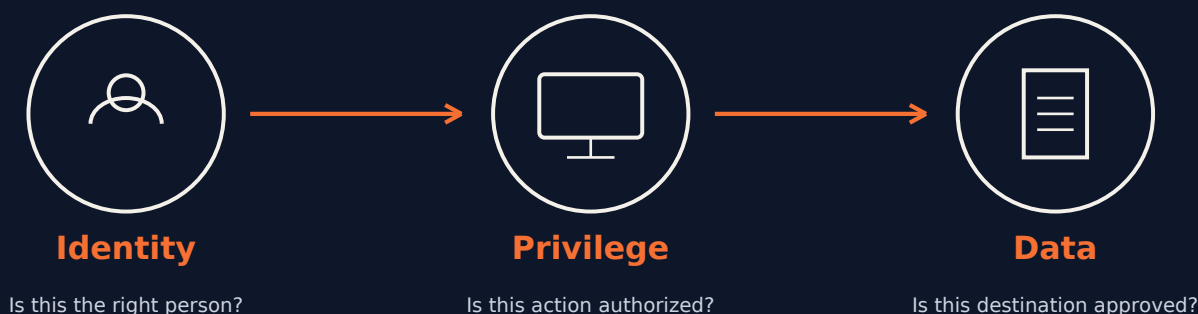
A person may collect harmless fragments from several coworkers that reveal a sensitive whole. Another may become the sole owner of a critical process and resist backup coverage. Watch for requests timed to holidays, shift changes, incidents, or launches, and repeated use of unnamed executives to discourage verification.



WHAT SYSTEMS MAY SHOW

Follow the access and the data

Technical alerts are leads. Context determines their meaning.



Compare an alert with the person's role, approved work, usual pattern, destination, and explanation. A late login may reflect on-call work. A bulk download may be an authorized migration. Verify before assigning intent.

Identity and privilege

Review unexpected devices, apparent impossible travel, repeated resets, new multifactor authentication (MFA) factors, and dormant accounts returning to use. Check for approved travel, device replacement, or support activity. Unrequested elevation, new accounts, group changes, or disabled logging need a matching authorization.

Movement and persistence

Bulk downloads, compressed archives, staged data, removable media, personal cloud storage, and external forwarding can expose information. Confirm the business purpose and destination.

Remote tools, mailbox rules, tokens, and alternate accounts may support legitimate automation—or continued unauthorized access.

Discovery and evasion

Searching for credentials, restricted projects, or monitoring gaps deserves context. Log deletion, security disablement, split transfers, and unexplained channel changes also merit review. Check whether approved testing, an audit, or troubleshooting explains the activity.

Remove unnecessary opportunity

Use phishing-resistant MFA for privileged and high-impact workflows. Do not reset identity on the strength of caller ID, biographical details, or a familiar voice. Separate payment, access, export, and production-change approvals.

Limit the duration of elevated access, review entitlements, revoke promptly, and protect logs. Tune data controls to business roles under privacy governance. Broad employee surveillance is not a substitute for a defined security purpose.

THE IP EXPOSURE MAP

Know your intellectual property

Protect the information that creates business advantage.

Intellectual property is not limited to finished products or source code. A company's sensitive knowledge may sit in designs, formulas, experiments, failed approaches, manufacturing tolerances, pricing methods, customer strategy, research notebooks, or an unreleased creative asset.

Name the asset and its owner

"Engineering data" is too broad to manage. Identify the particular repository, drawing set, model, formula, or process that matters. Assign a business owner who can explain why it is valuable and approve a legitimate use. Identify the systems that store it and the copies created by collaboration, testing, support, and backup.

Confidential information and a legally protected trade secret are not interchangeable labels. The legal classification depends on applicable law and facts. Have counsel advise on protections and agreements; do not assume a confidentiality stamp settles the issue.

Trace the useful fragments

An outsider may not need the whole design. A test result, a manufacturing setting, and a list of unsuccessful approaches can materially shorten development. Consider what a recipient could infer when several permitted disclosures are combined.

Map the life of a copy: creation, review, export, partner use, storage, and deletion or return. Include personal repositories, collaboration links, support attachments, service accounts, and subcontractors where relevant. A controlled original does little good if an unrestricted working copy remains elsewhere.

Reduce exposure without stopping work

Share the smallest useful subset. Prefer synthetic test data, limited drawings, interfaces, or a controlled workspace when they meet the task. Separate read access, bulk export, modification, and administration. Each permission enables a different kind of harm.

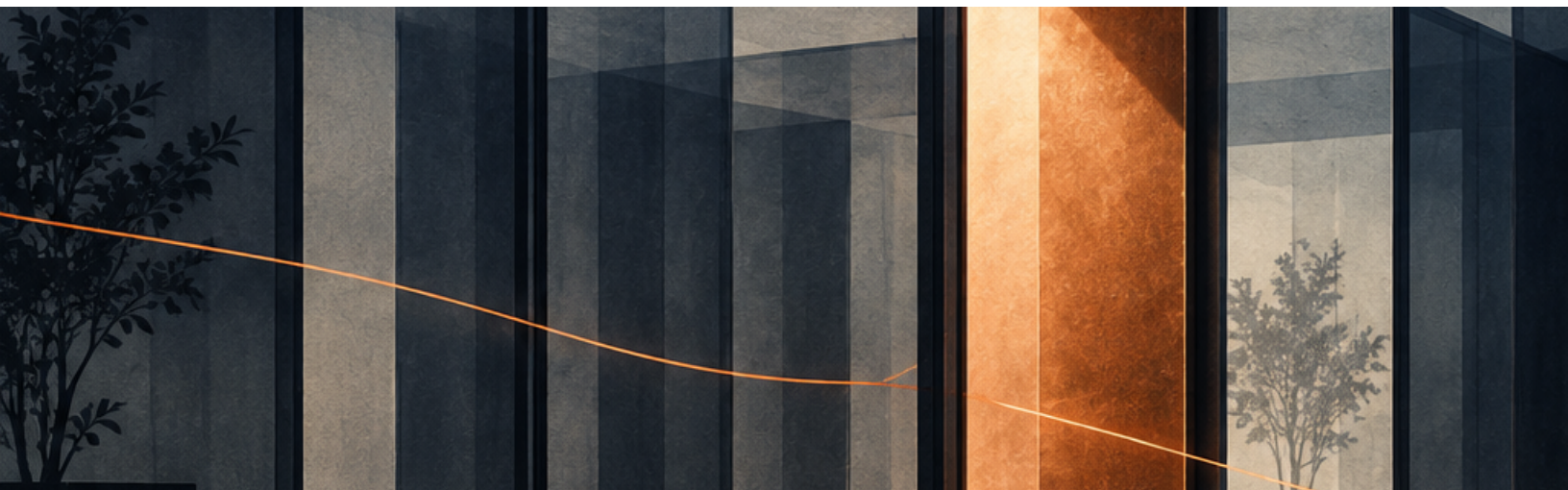
Worked example: a supplier troubleshooting a connector may need its dimensions and test results, but not the entire product design history. Ask the engineer and supplier to define the task before granting access to the whole project folder.



THE EXTENDED WORKPLACE

Access beyond the front door

A uniform, a badge, or a contract does not authorize every action.



CONCEPTUAL EDITORIAL ILLUSTRATION

Someone carrying equipment may follow a group through a controlled door or claim a badge has failed. Follow the site's challenge policy and direct them to reception or approved badge recovery. Keep yourself safe; do not pursue or restrain unless trained and authorized.

Check identity and scope

For a technician or delivery, verify the work order, sponsor, identity, and exact task. Branded clothing, tools, confidence, and familiar names are not sufficient. Loaned badges, photo mismatches, unexpected locations, or pressure to skip receiving controls should be reported.

A legitimate provider may ask for adjacent rooms, systems, or data. Return to the agreed purpose and the access owner. Record unexplained photography, door testing, or questions about security routines from a safe position without assuming motive.

Apply the same discipline remotely

Check identity continuity across hiring, interview, onboarding, device delivery, payroll, and access. Pause unexplained equipment rerouting or remote-access requests during setup. Independently verify changes to banking details, domains, support contacts, ownership, or staffing.

Every third-party connection needs a named owner, defined purpose, expiry, and review. When the relationship ends, remove accounts, tokens, integrations, devices, badges, and retained data according to policy.

Public settings also deserve care. Conferences, airports, hotels, restaurants, rideshares, and online communities can expose nonpublic projects, incidents, travel plans, or security arrangements to an unknown audience.

PARTNER AND SUPPLIER RISK

Third-party access has a life cycle

Every relationship needs an owner, a boundary, and an ending.

A third party may be a supplier, customer, consultant, managed service provider, research collaborator, or subcontractor. Some need information; others need a session, an integration, or physical entry. Treat those as specific access decisions rather than a single yes-or-no judgment about whether a company is trusted.

Before access is granted

The business sponsor should describe the task, required information, intended users, duration, and consequence of misuse. Confirm who may delegate or subcontract the work. Security and IT should translate the task into permissions; Procurement and Legal should address relevant contractual obligations. [4]

An agreement should reflect the work: permitted use, confidentiality, onward sharing, incident notification, return or deletion, and review rights as appropriate. Contract language and technical restrictions do different jobs. Neither replaces the other.

While the work is active

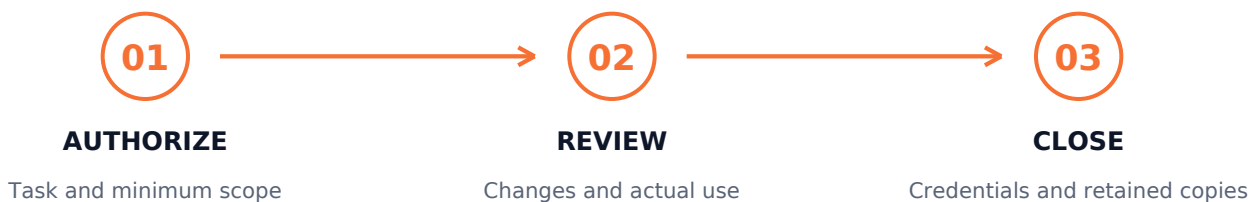
Use named identities where practical, approved devices or workspaces as appropriate, and time-limited access. Know how emergency support is authorized and who can approve an exception. Review actual use against the task, not simply whether the account still belongs to a valid vendor.

Reassess when personnel, ownership, domains, subcontractors, locations, or scope change. A new support engineer should not silently inherit every permission of the previous person. A purchase order renewal is not an automatic justification for expanded technical access.

At the end of the relationship

Revoke sessions, accounts, tokens, integrations, badges, and shared secrets as applicable. Address copies already delivered, legal retention needs, and agreed return or deletion. Record what was completed and what remains uncertain.

Worked example: cancelling a contractor's email account does not necessarily revoke a repository token or a cloud integration. The access inventory must include machine credentials as well as people. The relationship owner should verify closure with the relevant technical and business owners.



CONTROLS IN PRACTICE

Design access around the task

Ask what each permission allows the recipient to do.

Start with a concrete request: “The provider needs to diagnose a defect in one module for two days.” Work backward from that task. A broad project account may be convenient, but convenience alone does not explain why the provider needs unrelated repositories or an unlimited export capability.

Distinguish three decisions

Authentication establishes confidence in the identity using an account. Authorization determines what that identity may do. Business purpose explains why the action is needed now. A strong answer to one does not supply the other two. Current NIST identity guidance explains authentication and authenticator lifecycle considerations. [3]

Give view, edit, download, administration, and onward-sharing rights deliberately. A read-only account can still expose valuable information; it prevents alteration, not necessarily copying. Conversely, a support administrator may change a system without needing routine access to confidential design content.

Match the safeguard to the loss

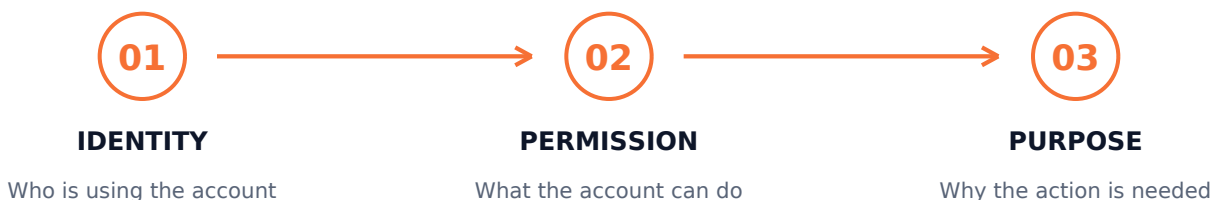
For sensitive review, a managed workspace may reduce uncontrolled copies. For administration, use approved access windows, session records where lawful, and rapid revocation. For a sensitive export, require the asset owner’s approval and an approved destination. Logging should answer who acted, what changed, and which object was involved.

Watermarks and audit records may help attribution, but they do not make disclosure impossible. A nondisclosure agreement cannot stop a live session. Avoid describing any one safeguard as complete protection.

Test the boundary

Before granting access, ask a simple set of questions: can this identity reach a neighboring project; can it export more than the task needs; can it invite another user; and will it still work after expiry? Test only through authorized procedures.

An exception needs an owner, reason, compensating safeguards, and a review or expiry time. Record the risk accepted by the authorized decision-maker. Do not let a temporary launch workaround become the permanent design by default.



PRIVATE SECTOR APPLICATIONS

What could the business lose

The useful indicator is the one connected to a meaningful consequence.

The same request can carry very different consequences in different workplaces. Translate this handbook into the assets and pressures your employees encounter, rather than relying on generic phishing examples.

Information and intellectual property

Technology and media companies protect code, credentials, product plans, user data, and creative work while managing launch pressure and remote access. Professional services protect client files and privileged communications across travel and temporary teams. Research and education balance collaboration with protection of labs, research, grants, and student records.

Operations and continuity

Manufacturers protect designs, formulas, production systems, and safety controls during maintenance and downtime. Energy and infrastructure firms must account for dispersed sites, remote access, overrides, and operational technology. Health care adds urgent clinical needs, patient safety, medication, shared devices, and vendor equipment.

Money and public access

Financial services face payment urgency, account recovery, trading information, and executive impersonation. Retail and hospitality combine payment and loyalty systems with guests, inventory, deliveries, seasonal staffing, and publicly accessible premises.

Make the assessment local

Name the five to ten assets whose loss or disruption would cause the greatest harm. Map who can reach them directly, through another person, through a provider, or through a physical route.

Ask where business pressure most often produces a shortcut. Build realistic reporting examples around those moments. Practice a scenario each quarter, then fix the weakness it exposes. A useful exercise changes a process, not just a training completion score.



Information

Code / research / client files



Operations

Production / care / continuity



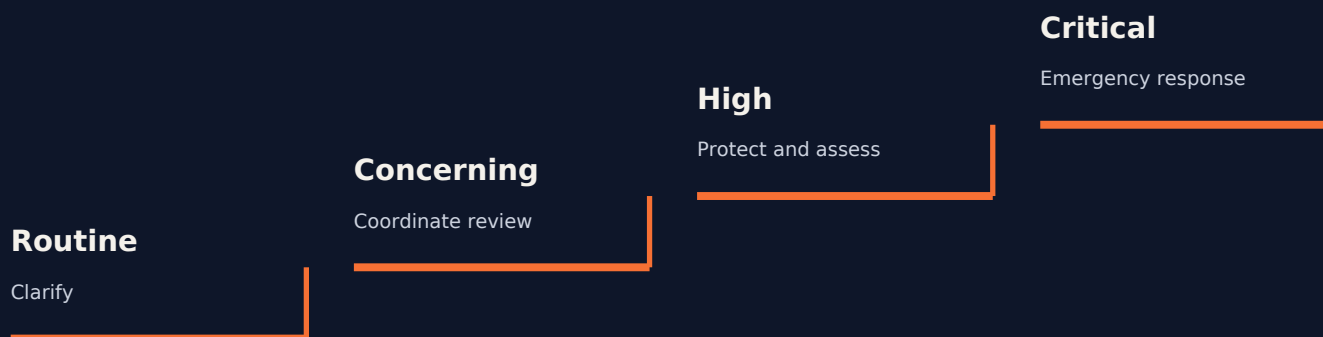
People and value

Safety / payments / property

A FAIR DECISION PROCESS

Escalate the facts, not the fear

Employees report. Authorized teams assess and decide.



Managers document and seek help; an authorized multidisciplinary team assesses. Keeping those roles separate protects both the company and the individual. Restrict information to people who need it for a legitimate response.

Start with a useful intake

Record exactly what happened, when, and where. Use direct quotes and identify the system, account, device, or location. Name the person, asset, or process that could be affected, and distinguish first-hand observations from allegations.

Check whether the activity fits the role and has approval. Is this a single event or a repeated pattern? What records, witnesses, or related activity support it? Consider a credible benign explanation as well as the concern.

Ask immediately about danger, active compromise, ongoing loss, and evidence at risk. Identify the least intrusive temporary step that adequately protects people and assets. Assign an owner and a review date.

Match response to consequence

Routine: clarify an ambiguous, low-impact event and document the explanation. Close it when resolved. **Concerning:** refer repeated bypass attempts, unexplained access, or suspicious requests for coordinated review.

High: targeted collection, concealment, significant exfiltration, or threat-related behavior may need immediate protective controls and formal assessment. **Critical:** imminent harm or active destructive activity requires emergency response; confirmed compromise activates incident response.

These categories guide coordination; they are not numerical predictions of a person's intent. Reassess restrictions as facts develop, restore access when justified, and record the reason for the decision.

INTAKE WORKSHOP

Write an actionable report

A worked example of separating evidence from inference.

Fictional training example: a project manager sees an engineer move documents to an unfamiliar cloud folder after announcing a departure. There is no immediate safety threat. A poor report says, “Alex is stealing our designs because Alex is leaving.” That statement supplies an accusation before establishing the facts.

A useful first report

“At 16:20 on 8 June, the project audit view showed account A17 exporting files from the restricted design folder to an external sharing destination. I do not know whether a transfer was approved. The account is assigned to Alex, whose departure is scheduled for Friday. I preserved the audit reference in the incident system and have not contacted the recipient.”

This report names the observation and limits. The departure is relevant to access review, but it does not prove intent. The destination may be an approved partner workspace; the account could also have been compromised. An authorized reviewer checks those possibilities.

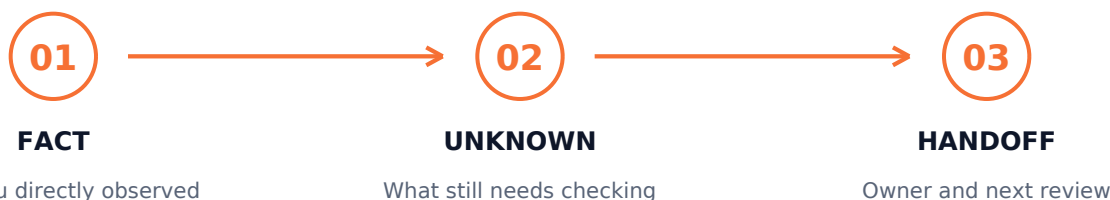
What the receiving team asks next

Which files and versions were involved? Who owns them? Does the destination match an approved recipient? Does a ticket or project record explain the export? Are sessions still active, and is transfer continuing? Is the account activity consistent with the assigned person’s device and authentication history?

The team should preserve relevant records and decide whether to pause the transfer or restrict access. The manager should not copy the entire repository into email “for evidence,” broadcast the allegation, or confront Alex before coordinating the response.

Close the loop

Record the owner, next action, and review time. If the export was legitimate, document the basis for closure and correct any process ambiguity. If concern remains, state exactly which question is unresolved. A report is successful when it enables a defensible decision, including a decision that no misconduct occurred.



FIRST ACTIONS

The first few minutes

Protect people, limit exposure, and preserve what responders need.



IMMINENT HARM: MOVE TO SAFETY AND CONTACT EMERGENCY SERVICES

A suspicious message or call

Stop before clicking, replying, disclosing, or approving. Keep the original message or voicemail, the sender or number, and the time. Verify through an established number, known directory, official ticket, or face-to-face contact. Report promptly and say immediately if credentials, data, money, or an MFA approval were exposed.

A reset or account recovery request

Require the approved ticket and identity-proofing method. Caller ID, employee details, a familiar voice, and a manager's name are not proof. Do not send codes to an unverified number or enroll an unverified authentication factor. Record repeated attempts, pressure, bribery, threats, and requests aimed at administrators.

Suspected data removal

Notify Security or incident response quickly. Preserve alerts, file paths, timestamps, devices, accounts, and relevant access records through authorized procedures.

Do not confront the person or search personal property. Avoid overwriting logs or unnecessarily alerting an actor; responders decide containment, and stopping immediate harm takes priority.

An unknown person in a controlled area

Follow the site's safety and challenge policy. Offer help and direct the person to reception or the named sponsor. Report their location, direction, appearance, time, claimed identity, and relevant companions or vehicle. Do not pursue or restrain unless trained and authorized.

Imminent harm

Move to safety and contact emergency services or site security. Share the location, exact threat, target, timing, and known weapons information. Do not delay to gather evidence or attempt negotiation unless trained and directed.

RESPONSIBLE RESPONSE

Preserve evidence and privacy

Collect what is needed through authorized procedures.

Evidence can be lost through well-intended action. Forwarding a suspicious message may remove context; opening a file may change a timestamp; copying sensitive material into a personal folder creates another exposure. Employees should preserve what they already have and follow the designated reporting route.

Give responders the original context

Record the original source, date and time including the time zone where known, account or device identifier, location, and actions already taken. Screenshots can help show what was visible, but they may not preserve full message headers, logs, or underlying records. Authorized responders decide which originals and system records to retain.

Keep a record of who collected an item, how it was handled, where it is stored, and who accessed it. Do not modify an original merely to make it easier to read. Qualified responders should use appropriate forensic methods when required; employees are not expected to perform a forensic examination.

Limit collection to the concern

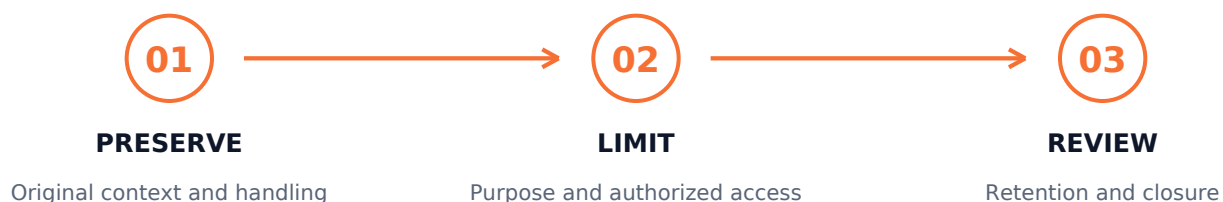
Define the purpose, scope, authorized reviewers, and retention requirements before expanding a search. Employment, privacy, labor, and evidence rules vary. Legal and Privacy should guide the process, including any preservation duties. This handbook does not authorize monitoring, searches, or access to personal accounts.

Share details on a need-to-know basis. Avoid informal watchlists, rumor channels, and speculative character descriptions. Keep support needs distinct from investigative conclusions, and protect those who make good-faith reports.

Contain without destroying the record

If loss or danger is active, protection comes first. The response lead should coordinate containment with preservation where feasible and document unavoidable tradeoffs. Do not delay an emergency to perfect the evidence.

Teaching point: preservation is not “save everything forever.” It is retaining the relevant material, under proper authority, in a way that preserves its reliability and respects applicable obligations.



LEADERSHIP IN UNCLEAR SITUATIONS

A manager's first responsibility

Address the work behavior and bring in the right help.

Managers should maintain standards, make reporting safe, and ask for help early. They should not conduct a private investigation. Before speaking to someone about a serious concern, coordinate with the authorized team if the conversation could increase danger, destroy evidence, or compromise a response.

When a management conversation is appropriate

If there is no immediate danger or suspected crime, begin neutrally: "On Tuesday and Thursday, you used a personal file service after the approved transfer was denied."

Explain the impact: "That created an unapproved copy of restricted project material."

State the expectation that project data remain in approved repositories. Then ask what work need or obstacle led to the decision. Listen without promising that the explanation will end the review. Offer a compliant method and agree on a correction and follow-up.

Keep the boundaries clear

Write factual notes and apply the process consistently. Protect reporters from retaliation. Do not diagnose motive or mental health, promise absolute confidentiality, circulate rumors, or leave unnecessary access in place simply because someone is trusted.

Make departures routine

Coordinate offboarding across the manager, HR, IT, Security, Legal, and Facilities. Inventory accounts, privileges, devices, keys, badges, tokens, repositories, forwarding rules, shared secrets, vendor access, and physical storage.

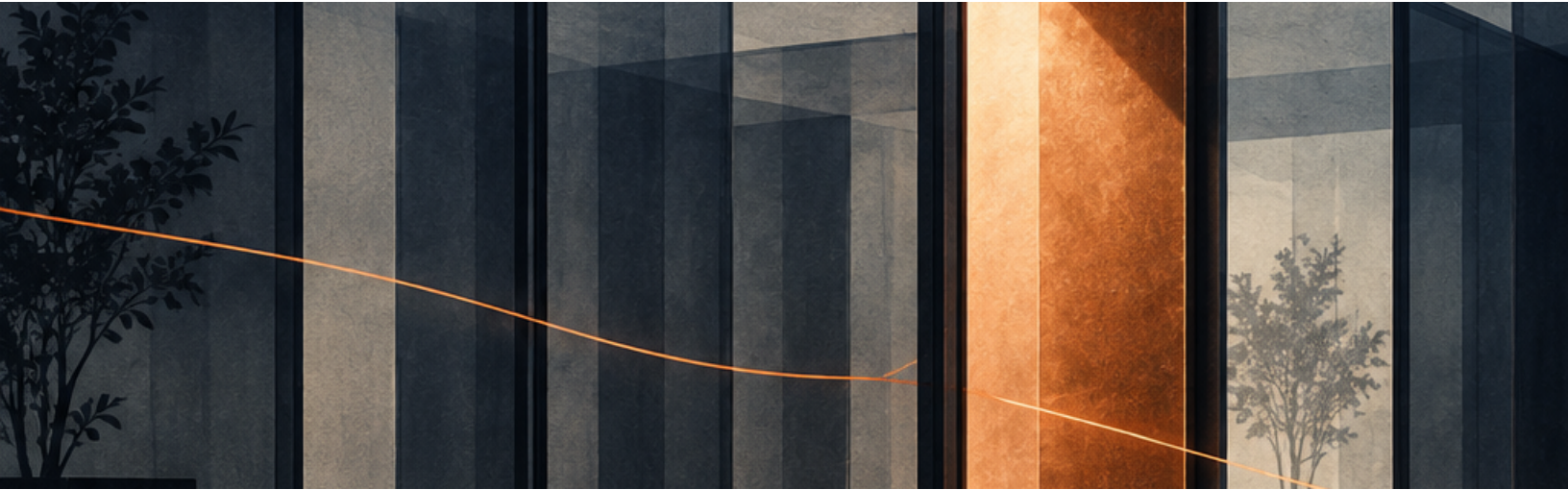
Agree on timing and verify completion. Remind the departing person of continuing obligations without making accusations. A standard process is easier to defend and less likely to miss a critical connection than an improvised response to a particular individual.



CASE STUDY ONE

An insider takes AI trade secrets

Google and Linwei Ding / Case status reviewed 24 September 2026



CONCEPTUAL EDITORIAL ILLUSTRATION

According to the Justice Department's account of the trial evidence, Google engineer Linwei Ding took more than 2,000 pages of confidential AI information from the company's network to a personal cloud account between approximately May 2022 and April 2023. The material concerned Google's AI computing infrastructure. [6]

While still employed, Ding pursued roles in two technology ventures outside Google, including a company he was founding. DOJ described statements to investors about copying and modifying Google's technology. In December 2023, shortly before resigning, he downloaded the stolen information to his personal computer. [6]

The legal outcome matters

A January 2026 jury verdict included trade-secret theft and economic-espionage counts. In August, the judge set aside the espionage convictions while leaving the trade-secret verdicts in place, according to Reuters.

The distinction was whether the required government-benefit element had been proved. [7]

Courthouse News reported that on 1 September 2026 Ding received a sentence of 12 months minus one day, with two years of supervised release. This handbook does not present the overturned espionage counts as standing convictions. [8]

What makes this an insider case

The documented conduct involved an employee removing employer information while pursuing competing business activity. The lesson concerns access, destination, purpose, and evidence. Nationality is not a detection criterion. The next page translates the facts into questions a private company can use without claiming that every suggested control was absent at Google.

CASE STUDY ONE DEBRIEF

Debrief the insider case

Control lessons are recommendations, not additional findings about Google.

The central boundary was between permitted use of company information and removal for an outside purpose. Technical competence and legitimate access did not authorize personal retention. A company needs controls that continue to make sense when the account holder is a capable, trusted employee.

Ask about the destination

Can the company distinguish approved collaboration from a transfer to personal storage? Does an alert identify the sensitive material and receiving account, or merely report a large upload? Could a reviewer check the underlying work approval without collecting unrelated personal information?

Volume alone is a weak story. A small but complete design may be more damaging than a large collection of routine files. Asset owners should help prioritize what would give another organization a meaningful advantage.

Ask about competing purpose

Does policy clearly explain which outside work and conflicts must be disclosed? Is there a usable route for asking whether a consulting opportunity is acceptable? An undeclared relationship may justify review under policy, but a company still needs evidence of the conduct at issue.

Do not treat the case outcome as a license to profile employees. Similar access decisions should receive similar review regardless of an employee's nationality, background, or seniority. An investigation should test account compromise and authorized work as alternative explanations where relevant.

Ask about departure and closure

Can the company review necessary access and active transfers during an ordinary departure without assuming wrongdoing? Can it revoke tokens and sessions, preserve relevant records, and avoid circulating an accusation before assessment?

Discussion: choose one preventive safeguard, one detection question, and one response action for a sensitive repository. A reasonable set is task-based access; verification of an unusual destination; and a proportionate, authorized pause while the transfer is assessed. Explain what each action would and would not establish.

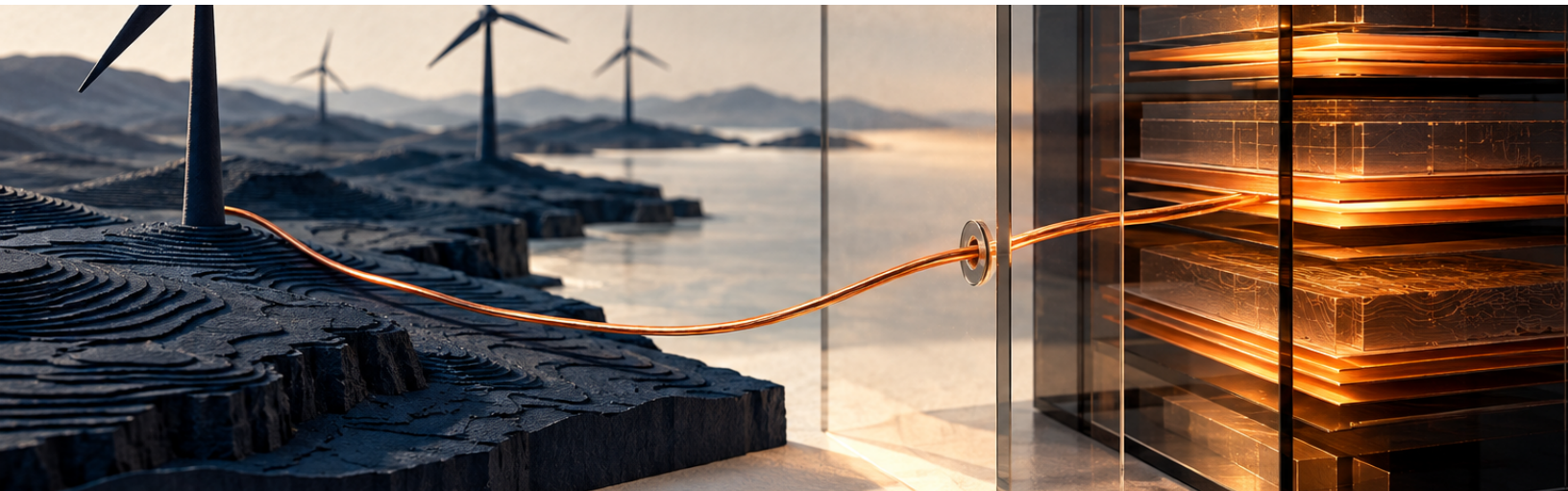
Source boundary: documented case facts are on page 21. The questions here are CCI's analysis, not claims about Google's internal controls or a prediction that a particular safeguard would have prevented the theft.



CASE STUDY TWO

A partner takes proprietary code

AMSC and Sinovel / Historical case: 2011 conduct, 2018 conviction



CONCEPTUAL EDITORIAL ILLUSTRATION

Sinovel was a commercial customer of AMSC, whose technology included software regulating electricity from wind turbines to the grid. At the time of the theft, the relationship involved more than \$800 million in contracted products and services. [9]

According to DOJ's trial account, Sinovel persuaded an AMSC Windtec engineering employee to leave, join Sinovel, and steal source code. The employee secretly downloaded code from an AMSC computer in Wisconsin to a computer in Austria in March 2011. Sinovel used software compiled from the stolen code in turbines, including installations in Massachusetts. [9]

The relationship was part of the pathway

A federal jury convicted Sinovel in January 2018 of conspiracy to commit trade-secret theft, theft of trade secrets, and wire fraud.

At sentencing in July, the court found AMSC's losses exceeded \$550 million and imposed a \$1.5 million fine. DOJ separately described a restitution settlement; the loss finding and fine were different measures. [10]

Why this case belongs here

This is third-party acquisition of IP through a recruited insider. It is not a claim that an ordinary supplier account was hacked or that Sinovel had authorized access to AMSC's source repository. The distinction shows why partner risk and insider risk can overlap.

The case is older than the Google vignette, but it offers a clear, adjudicated example of a business relationship becoming an IP-theft pathway. The next page examines access boundaries and collaboration choices without inventing missing details about AMSC's controls.

CASE STUDY TWO DEBRIEF

Debrief the third-party IP case

A legitimate relationship does not authorize every use of information.

Companies often define third parties too narrowly as IT vendors. A customer, distributor, joint-development partner, or research collaborator can also receive valuable knowledge. Commercial importance should inform continuity planning; it should not silently expand the information that the recipient is entitled to obtain.

Map the whole route to knowledge

List the interfaces through which the partner interacts with the business: engineering support, demonstrations, workshops, shared repositories, on-site visits, and individual experts. Consider both formal access and requests directed to employees outside the agreed workflow.

A partner may need a functioning component without needing the source code that created it. Ask whether documentation, an interface, a limited data set, or a supervised session can satisfy the task. Some work genuinely requires deeper sharing; in that case, make the decision explicit and protect it accordingly.

Recognize the overlap

In the documented case, the external company obtained code through an employee. Reviewing vendor accounts alone would not describe that route.

Companies should also provide clear conflict-of-interest rules, a safe route for reporting recruitment or payment tied to restricted information, and checks on sensitive exports.

An ordinary job offer is not wrongdoing. The meaningful distinction is whether someone is being asked to take information, conceal an unauthorized transfer, or act outside a permitted business purpose. Apply that distinction consistently.

Plan for commercial pressure

If a major partner requests a sensitive exception, who can approve it? What does the partner need to complete the task, and what could be withheld or substituted? Who records the decision and verifies access closure?

Discussion: a key customer insists that only the complete source repository will solve a support problem. The responsible first step is a joint technical scoping review and escalation to the asset owner. Neither the customer's importance nor the existence of an agreement by itself establishes necessity.

Source boundary: this page presents CCI recommendations. It does not claim that the public record establishes which access controls AMSC had or lacked.



PRACTICE AND DISCUSSION

Exercise one the engineer

A fictional tabletop for managers, IT, HR, and Security.

Set aside 25 minutes. Select a facilitator, decision-maker, and note-taker. Use your own reporting contacts, but do not access real employee records. The purpose is to rehearse decisions and identify unclear responsibilities.

The opening situation

An engineer will leave in five days. A monitoring alert shows an unusually large export from a design repository to an external workspace. The engineer is responsible for preparing a customer handover. A manager says, "I trust this person; just close the alert."

Pause for discussion. What is established? What is unknown? Which approval or recipient record would help? Who can temporarily pause the export, and what business impact would that create? Write the next decision and its owner before requesting more facts.

The second development

The workspace name resembles a known customer's name, but the recipient domain differs. No matching transfer approval appears in the project ticket. The engineer says a customer contact requested the workspace and provides the email. The alert does not establish whether anyone downloaded the files.

Discuss what must be independently verified. Do not treat a lookalike name as proof of fraud or the engineer's explanation as proof of authorization. Identify how responders would preserve the original email and sharing records and limit further exposure.

The third development

The real customer confirms that the contact was impersonated. The engineer believed the request was legitimate. A sharing link remains active. Decide how to revoke it, check access, notify the right people, and support the employee without promising a particular investigative outcome.

Record the learning

List the control failure, the detection opportunity, and the response improvement. Avoid ending with "train employees better." Name a specific change to external-sharing approval, recipient verification, or link expiry. Compare your reasoning with page 27.



PRACTICE AND DISCUSSION

Exercise two the urgent supplier

A fictional tabletop for Engineering, Procurement, IT, and Security.

Set aside 25 minutes. A supplier is diagnosing a manufacturing fault before a launch. Its contract covers one component. A replacement engineer requests a complete design archive, a shared support login, and permission to use a subcontractor's file-transfer site. The project lead says delay will be expensive.

First decision

Which part of the request is necessary for the task? Identify who owns the design archive and who may approve supplier users, onward sharing, and an exception. Explain why a valid contract does not settle those separate decisions.

Propose a minimum useful alternative: the relevant drawing revision, a limited test result, or a controlled troubleshooting session. If none will work, define what technical evidence is needed to justify a broader disclosure.

The second development

The supplier confirms the engineer is genuine, but says the subcontractor is new and has not yet completed its customer approval process. The shared login has been used by three people. A previous support token remains active from a closed assignment.

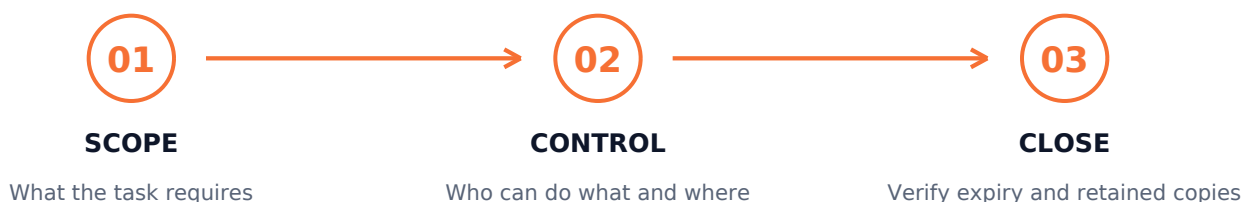
Discuss attribution and access closure. A genuine engineer can still request an unauthorized action. Decide which access can safely continue, which should pause, who will review the subcontractor, and how to remove the stale token without disrupting unrelated work.

The third development

Engineering finds that a limited diagnostic package will resolve the issue. The supplier accepts a named account in the approved workspace for 48 hours. Define the approval record, access expiry, logging, and follow-up needed to verify that the exception actually ended.

Record the learning

Your exercise output should be a short access decision, not a broad statement that the supplier is safe or unsafe. Include purpose, data scope, named recipients, destination, duration, approval, and closure owner. Compare your reasoning with page 27 and test whether your real onboarding process captures those fields.



FACILITATOR GUIDANCE

Debrief the two exercises

Evaluate the reasoning and the handoffs, not just the final answer.

In exercise one, the initial alert does not prove deliberate insider theft. A legitimate handover and the approaching departure are context. The later facts reveal manipulation of a trusted employee. Good reasoning preserves multiple explanations until the evidence distinguishes them.

What a strong response shows

The team identifies the asset owner, checks the recipient independently, preserves the original message and sharing records, and uses an authorized, proportionate restriction while exposure is assessed. Once impersonation is confirmed, responders revoke active access and determine what was actually reached. They do not assume that link creation equals download.

The employee's prompt cooperation is useful evidence and a reason to support early reporting. It does not remove the need to establish exposure. A control improvement might require recipient validation for sensitive external sharing and an expiry that is enforced automatically.

In exercise two, identity verification resolves only one question. The engineer can be genuine while the requested archive, shared login, and new transfer site remain outside authorization. The team should narrow the task, confirm recipients and subcontractors, use attributable access, and verify closure.

Questions for the facilitator

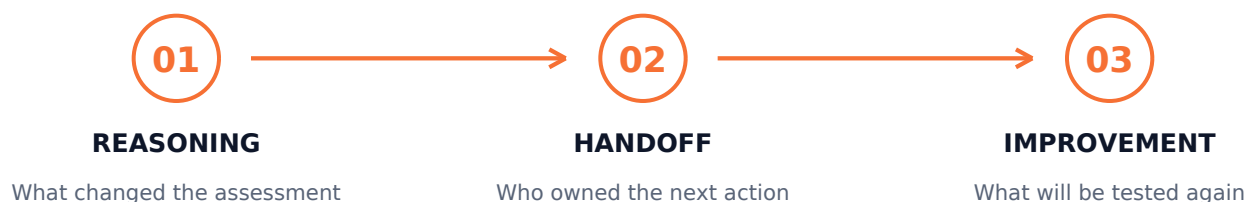
Did participants identify an action owner and a decision deadline? Did they explain which evidence could change the decision? Did anyone assume seniority, trust, a contract, or a familiar name replaced approval? Did they preserve business continuity while reducing exposure?

Watch for the opposite failure as well: collecting irrelevant personal information, labeling an employee a thief, or shutting down a whole supplier relationship without considering a narrower protective step.

Turn discussion into a change

Record one improvement per weakness, with an accountable owner, due date, and method of verification. Repeat the scenario after the change. Completion means the process works under pressure, not that everyone attended the session.

These are model debriefs, not the only acceptable answers. Different organizations may choose different controls if they can explain the authority, consequence, evidence, and limits of their decisions.



PUT IT INTO PRACTICE

Turn awareness into practice

A first 90 days plan for owners, verification, and learning.

Use a ten-second pause

Who is asking, and how do I know? Verify through a separate trusted channel. Is the request normal for both roles? Confirm its purpose and authorization. Which control would this bypass? Return to the approved process and take only the minimum safe action.

Make reporting easy

A useful report includes the date, time, location, system, account, device, and channel. Preserve exact words or observable actions and the original contact. Identify who or what may be affected, related records or witnesses, verification attempts, and actions already taken. Flag immediate danger, active compromise, or continuing loss.

Days 1 to 30

Name accountable owners and publish reporting and emergency routes. Identify critical assets and high-risk workflows.

Review help desk identity proofing and payment verification. Employees should know where to turn before a suspicious request arrives.

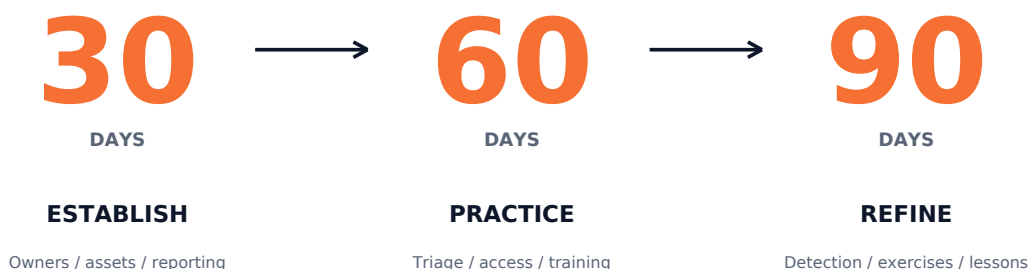
Days 31 to 60

Create multidisciplinary triage. Review privileged access and offboarding. Train managers, Finance, Reception, and the help desk using examples from their work. Run a scenario and assign corrective actions with owners and dates.

Days 61 to 90

Tune detection across relevant systems under privacy governance. Test response playbooks, review third parties, and track the improvements. Check that temporary exceptions have owners and expiry dates.

Measure reporting speed, response time, unresolved exceptions, access ownership, false-positive review, and completed corrective actions. Reward timely reporting and learning. Do not use raw report counts to label individuals or punish employees for raising concerns.



FIELD TOOLS

Two tools to use at work

Make the important information easy to capture.

A concise concern report

Write the date, time, location, and relevant system or account. Describe exact words or observable actions. Identify the source of each statement: direct observation, a record, or a report from someone else. State what is unknown rather than filling the gap with an assumption.

Name the person, asset, or process that could be affected. Include the original record location, relevant witnesses, verification attempts, and actions already taken. Flag immediate danger, active compromise, or continuing loss. Route the report through the designated system and record the receiving owner.

Useful closing sentence: “The unresolved question is whether this destination was approved; the asset owner is reviewing it by 14:00.” This is more actionable than “Please investigate urgently” with no decision or owner attached.

A third-party access decision

Record the business sponsor, asset owner, provider, named users, and any approved subcontractors. Define the task, specific information or system, allowed actions, approved destination, and duration. Separate ordinary access from export and administration rights.

Record who approved the decision and any exception. Identify the controls, review time, and person responsible for expiry. At closure, document credentials revoked, sessions ended, integrations removed, and how retained copies are being handled under the agreement and applicable obligations.

Put the tools where work happens

Add these fields to an existing ticket or incident workflow rather than creating a private spreadsheet of allegations. Keep reporting simple enough for employees to start without having every answer. The receiving team can obtain additional facts under the proper authority.

Before publishing locally, identify a normal reporting route, an urgent security route, and an emergency route. Test that someone receives each one. A well-written handbook cannot compensate for a reporting address that nobody monitors.



WORKING GLOSSARY

The language of insider risk

Use precise terms so teams can make the same decision.

Insider risk is the possibility of harm connected to authorized access, knowledge, or proximity. **Insider threat** concerns a person or activity that can use that position to cause harm. Terminology varies; define it locally without assuming every risk is intentional.

Indicator means an observable event or behavior worth checking. **Corroboration** means supporting evidence that strengthens an interpretation. Neither term means proof of motive or guilt.

Authentication establishes confidence in an identity. **Authorization** defines permitted actions. **Least privilege** limits permissions to the work required.

Multifactor authentication combines distinct kinds of authentication factors; it is not simply two passwords. [3]

Social engineering is manipulation intended to cause an unsafe action or disclosure. **Pretext** is the story used to make the request credible. **Independent verification** checks through an established route that does not depend on the suspicious request's contact details.

Intellectual property covers legally recognized forms of protected creation or knowledge. **Confidential information** is information an organization restricts.

Trade secret is a legal category with requirements that depend on applicable law; obtain qualified advice rather than applying the label automatically.

Exfiltration is unauthorized removal or transfer of information. **Persistence** is continued access, such as through an account, token, or integration.

Containment limits ongoing exposure or harm while a response proceeds.

Third party includes external suppliers, service providers, customers, partners, and collaborators. **Subcontractor** is another organization or person engaged to perform part of the work. An approved third party does not automatically confer approval on every subcontractor.

False positive is an alert that does not represent the condition being sought. **Near miss** is a situation that could have caused harm but did not, or whose harm was limited. Both can reveal a process worth improving.



REFERENCE

Sources and reading notes

Source review date 24 September 2026

The references below separate general defensive guidance from the records used for the two case studies. Numbered references appear where a passage relies on a particular source. Case debriefs and fictional exercises are CCI's educational analysis.

General guidance

[1] CISA. Insider Threat Mitigation Guide and program resources. Open source.

[2] Carnegie Mellon SEI. Common Sense Guide to Mitigating Insider Threats, Seventh Edition (2022). Open source.

[3] NIST. SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management. Open source.

[4] NIST. SP 800-161 Rev. 1, Update 1: Cybersecurity Supply Chain Risk Management Practices. Open source.

[5] NIST. IR 8276, Key Practices in Cyber Supply Chain Risk Management (2021). Open source.

Using these sources

CISA and SEI provide broader insider-risk program guidance. NIST identity guidance helps teams distinguish authentication from access authorization. NIST supply-chain publications provide context for supplier and dependency management.

Federal guidance is a reference framework here, not a statement that every requirement applies to every private company. Determine applicability with the appropriate owners and advisors. A framework does not replace a risk assessment of your own assets and relationships.

For the Google case, the January DOJ release describes the original verdict. The August and September reporting is necessary to understand the later outcome; do not cite the January headline alone as the current legal status.



REFERENCE AND ABOUT CCI

Case references and CCI

Copperhead Consulting Inc / Expanded learning edition

[6] US Department of Justice. Ding trial account and January verdict, 30 January 2026; read with sources 7 and 8. Open source.

[7] Reuters. Partial overturning of Ding verdict, 20 August 2026. Open source.

[8] Courthouse News Service. Ding sentencing report, 1 September 2026. Open source.

[9] US Department of Justice. Sinovel conviction and account of trial evidence, 24 January 2018. Open source.

[10] US Department of Justice. Sinovel sentencing, loss finding, and restitution, 6 July 2018. Open source.

About Copperhead

Copperhead Consulting Inc provides Protective Services, Investigations, and Risk Management. We help leaders protect people and assets, investigate concerns, and build security practices that work in daily operations.

copperheadci.com

Publication notes

Written by Joshua D. Tatro, Chief Operating Officer, Copperhead Consulting Inc. Expanded learning edition, September 2026. Adapt with Legal, HR, Privacy, IT, Security, and business owners. This is educational guidance, not legal advice or authority to conduct an investigation.

Review sources and case status before republication and at least annually. Update contacts and procedures whenever ownership or reporting routes change. Fictional exercises are labeled; conceptual AI-generated artwork does not depict actual people, premises, or events.

Copyright 2026 Copperhead Consulting Inc. Internal educational use with attribution permitted. All other rights reserved.



Protective Services



Investigations



Risk Management