PsySecure

AN ODSF GUIDE

MINIMIZE WHAT CAN BE KNOWN

AN EXECUTIVE GUIDE TO REDUCING THE PUBLIC INFORMATION THREAT ACTORS USE

While threat actors will certainly consider malware, the attack often begins at the reconnaissance stage.

FA1	FA2	FA3	FA4	FA5
DIGITAL FOOTPRINT REDUCTION	SOCIAL ENGINEERING DEFENSE	TECHNOLOGY EXPOSURE MANAGEMENT	EXECUTIVE EXPOSURE PROTECTION	CONTINUOUS MONITORING AND RESPONSE

Version 2026.06

CONTENTS

Executive guide to exposure controls that reduce attacker reconnaissance.

A practical playbook for reducing public-information attack paths, hardening recovery and identity, and keeping foundational controls owned after deployment.

BUILT ON THE ODSF FOCUS AREAS

OPENING THESIS

Minimize What Can Be Known

While threat actors will certainly consider malware, the attack often begins at the reconnaissance stage.

They map your executives, domains, vendors, job posts, exposed systems, leaked credentials, phone numbers, email patterns, public documents, social profiles, and recovery paths. That information becomes phishing, business email compromise, SIM swap, domain impersonation, credential stuffing, vendor fraud, invoice redirection, extortion, and targeted intrusion.

This guide is written for executive teams, founders, risk owners, CISOs, security leaders, and IT owners who want to reduce the information threat actors can use before it becomes a crisis.

This guide applies the OSINT Defense & Security Framework (ODSF): a practical methodology for reducing the public information threat actors can find, connect, and turn into leverage.

OPERATING PRINCIPLE

Threat actors start with reconnaissance. Reduce what can be found, imitated, recovered, redirected, or socially engineered.

ODSF FOCUS AREAS

FA1	Digital Footprint Reduction
FA2	Social Engineering Defense
FA3	Technology Exposure Management
FA4	Executive Exposure Protection
FA5	Continuous Monitoring and Response

psysecure.com/odsf

WHAT THREAT ACTORS DO WITH EXPOSURE

01
FOUND
Public records, profiles, and leaks are mapped into a target picture.

02
IMITATED
Domains, brands, and voices are copied to borrow your trust.

03
RECOVERED
Weak account-recovery paths turn into front doors.

04
REDIRECTED
Mail, money, and traffic are quietly rerouted.

05
ENGINEERED
People are pressured with detail that feels legitimate.

READER'S NOTE

How to Read This Guide

The executive view in each section explains the business risk in plain terms and why it matters to security leaders. The deeper guidance gives security, IT, GRC, and operations teams the detail to act.

You do not need to read the guide from beginning to end. If you are triaging, start with the controls that would result in the most risk reduction for the least operational disruption:

- Email authentication enforcement.
- Phishing-resistant MFA for privileged and high-risk users.
- SIM-swap-resistant account recovery.
- Enterprise password management.
- Registrar and DNS hardening.
- Browser security.
- Patching internet-facing systems on the CISA Known Exploited Vulnerabilities list.
- Credential-leak monitoring.
- External attack surface inventory.
- Executive OSINT footprint reduction.

If you are reading this during or after an incident, go to the "If it happens" steps inside the relevant section, then to **Section 16**, The Reactive Takedown Runbook. Return to the prevention guidance once the immediate response is under way.

A recurring theme runs through the guide: most security fundamentals fail because **nobody owns them after deployment**. The control exists, the vendor supports it, and the organization still fails because the control drifted, the exception became permanent, or the recovery path undermined the primary control.

Each numbered section opens with the ODSF focus areas it serves, FA1 through FA5. One tag, Foundation, marks the general security disciplines reconnaissance defense depends on: exposure reduction shrinks what threat actors can find, and the foundations decide what a threat actor can do with what still gets found.

CONTROL GUIDANCE

Every section should have an owner, a review cadence, and evidence that the control is still working.

Domain and Brand Impersonation

Executive view

Threat actors can damage your organization without ever breaching it. They register lookalike domains, create fake login pages, send believable email, impersonate support teams, run recruitment scams, redirect payments, or deceive customers and employees. This is what we call **The Breach Before the Breach**.

The business risk is the abuse of trust, and a convincing lookalike domain can turn **your brand** into the threat actor's infrastructure.

Leadership should expect the organization to monitor for lookalike domains, maintain a response process when abuse appears, and know which domains are important enough to protect more aggressively.

Deeper guidance

Threat actors register names that resemble yours and stand up content, email, login pages, payment flows, fake support channels, or recruitment scams under them. The common variants are predictable.

Typosquatting uses fat-finger errors: missing letters, doubled letters, adjacent-key swaps, singular versus plural, and common misspellings.

Combosquatting uses your real brand plus a plausible word, often with no character substitution at all: `acme-login.com`, `acme-secure.com`, `acme-invoices.com`, `acmesupport.com`. This is one of the most important patterns because the brand string is genuinely present, which defeats naive exact-match filtering.

TLD swaps use the same string under a different extension: `.com` becomes `.co`, `.net`, `.io`, a country-code TLD, or one of the newer generic TLDs.

Homoglyphs use characters or character combinations that look alike. These split into two different categories that are often conflated: IDN homoglyphs and ASCII confusables.

Technical note: Punycode and homoglyphs

Punycode is the ASCII-compatible encoding that makes internationalized domain names work. It appears with the `xn--` prefix. Because it supports legitimate internationalized domain names and can also appear around confusing labels, treat it as a useful signal to inspect rather than as a standalone verdict.

Modern browsers and many registries have reduced the simplest mixed-script attacks, where a single Latin letter is swapped for a look-alike from another script: a domain that reads as `acme.com` but uses the Cyrillic a (U+0430) in place of the Latin a looks almost identical and resolves to a different `xn--` address. Defenses still vary by vendor, locale, script policy, and confusability rules. More importantly, many protections apply in the address bar after navigation. Email bodies, anchor text, QR codes, chat messages, PDFs, and SMS messages can still display convincing Unicode text before the user reaches a browser warning.

ASCII confusables never touch the IDN or Punycode machinery. `rn` can read as `m`, capital `I` can read as lowercase `l`, `1` can read as `l`, `0` can read as `O`, and `vv` can read as `w`. These are pure ASCII, so browser IDN protections do not help. On phones, in sans-serif fonts, and in rushed approval workflows, they can be more convincing than exotic Unicode attacks.

The practical conclusion: do not treat pre-registering Unicode variants as your defense. Domain impersonation is primarily a monitoring, scoring, and response problem.

Defensive registration

Register the small set of obvious, high-value variants: the exact brand under the most important TLDs, the hyphenated form, singular and plural variants, and the one or two obvious typos. This is baseline insurance.

Do not confuse defensive registration with strategy. The permutation space is effectively unbounded. You cannot register every typo, homoglyph, TLD swap, combosquat, executive-name variant, product-name variant, and campaign-specific lure. Competent threat actors operate in the long tail.

Monitoring is the strategy

Monitor the registration and certificate surface continuously.

Certificate Transparency logs are one of the highest-signal sources. A phishing site that wants to look legitimate will often request a TLS certificate, and that certificate appears in public CT logs. Monitor for your brand, product names, executive names, high-value domains, and edit-distance variants.

Newly registered domain feeds catch domains before certificates appear. Passive DNS helps correlate infrastructure, hosting, name servers, and repeated threat actor patterns. WHOIS and RDAP changes can surface suspicious registration behavior, though privacy redaction limits the usefulness of registrant data.

Score the combination of signals. A same-day registration, a lookalike string, a short-lived domain-validated certificate, suspicious hosting, copied page content, mail exchange records, and brand-themed paths are much stronger together than any one indicator alone.

Use confusable matching in two layers: Unicode skeleton matching for IDN cases, and a separate ASCII confusable map for the common lookalikes that never become Punycode.

If it happens

Capture the evidence before anything changes. Screenshot the lookalike page, record the full URLs and timestamps, and pull the WHOIS or RDAP record, the TLS certificate from the CT log, the DNS records, and the hosting and name-server details. The page may disappear once you start reporting, so keep this package first.

Then move in parallel. Report the URL to browser and safe-browsing ecosystems and file abuse with the host and the registrar at the same time, since they are usually different parties. Warn customers and staff through your own verified channel: name the real domain, and give them a reporting path. If money moved, notify the bank, payment processor, and fraud team immediately. **Section 16**, The Reactive Takedown Runbook, holds the full sequence and the provider report links.

OWNERSHIP AND EVIDENCE

OWNER

Security operations, brand protection, or domain management owner.

REVIEW CADENCE

Continuous monitoring with monthly review.

EVIDENCE TO RETAIN

Lookalike-domain alerts, abuse reports, takedown requests, screenshots, DNS records, and certificate records.

KEY METRIC

Time from detection to containment.

Hardening Your Real Domains

Executive view

A lookalike domain can (and will) mislead people, and losing control of your real domain can disrupt the business.

Your primary domains are business-critical assets and must be treated as such. They support email, websites, customer trust, authentication flows, brand reputation, and sometimes revenue. Domain security deserves the same rigor as identity security.

Leadership should expect crown-jewel domains to have strong account protection, change controls, monitoring, and recovery procedures.

CONTROL GUIDANCE: A registrar setting becomes a business control only when access, approvals, alerts, and recovery are owned.

Deeper guidance

Registrar accounts should use phishing-resistant MFA wherever supported. At minimum, use strong MFA, a dedicated registrar email address, a password manager, strict access control, and alerting on login, contact, DNS, nameserver, and transfer changes.

Use registrar lock by default. For crown-jewel domains, use registry lock. Registry lock is operationally heavier because changes require additional out-of-band verification, but that friction is the point. Use it for domains whose loss would create material business harm.

Publish CAA records to restrict which certificate authorities may issue certificates for your domains. CAA reduces unauthorized issuance through compliant public CAs, though certificate-abuse defense still requires monitoring and response.

Enable DNSSEC where your registrar, DNS provider, and internal operations can support it safely. DNSSEC adds integrity protection for DNS answers, but it must be owned properly. Bad key rollover and poor operational discipline can create outages.

Monitor your own domains in CT logs. Unexpected certificates for your domains or subdomains may indicate shadow IT, vendor activity, dangling DNS, misconfiguration, or compromise.

For crown-jewel domains, document who can approve registrar, DNS, nameserver, and certificate changes. The approval path should not depend on one person or one inbox.

If it happens

The change records are the first thing to save. Export the registrar and DNS change logs, pull your certificate-monitoring records, and screenshot the altered records before you revert anything, because reverting overwrites the proof of what changed and when. Then take back the registrar account: reset the password from a known-good device, revoke other active sessions, and re-enroll phishing-resistant MFA. Check the account contacts, recovery email, and notification settings for anything the threat actor left behind.

Now restore control. Revert the malicious DNS or nameserver edit and rebuild the correct records from your last known-good zone. For an unauthorized transfer or a registry-lock bypass, work the registrar and registry recovery process, which needs out-of-band verification you cannot self-serve. Revoke any certificate the threat actor had issued through the issuing CA. Treat redirected mail or web traffic as credential capture, and warn affected users to reset what they entered. For lookalike infrastructure and customer alerts, follow **Section 16**.

OWNERSHIP AND EVIDENCE

OWNER

Domain owner, security operations, or infrastructure leader.

REVIEW CADENCE

Quarterly access review and continuous change alerting.

EVIDENCE TO RETAIN

Registrar access list, lock status, DNS change records, certificate monitoring, and CAA records.

KEY METRIC

Percentage of critical domains with registrar MFA, lock protection, and change alerting.

Email Authentication and Mail Trust

Executive view

Email remains one of the easiest ways to impersonate an organization. If threat actors can send mail that appears to come from your domain, they can target customers, employees, vendors, executives, finance teams, and partners.

Email spoofing creates phishing risk and a broader loss of trust in the organization's communications.

Leadership should expect the organization to know who is allowed to send email as the brand, block unauthorized senders, and monitor mail authentication health over time.

CONTROL GUIDANCE: DMARC creates value when it reaches enforcement without breaking legitimate business mail.

Deeper guidance

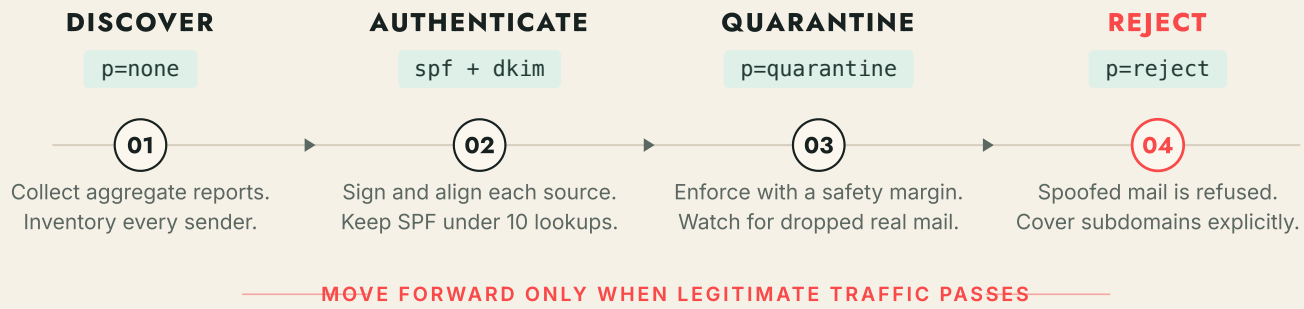
Email authentication remains one of the highest-ROI anti-spoofing controls.

SPF lists which systems may send mail for your domain. DKIM cryptographically signs outbound mail. DMARC ties SPF and DKIM to domain alignment, tells receivers what to do with mail that fails, and gives reporting on who is sending as you.

The common failure is DMARC stuck at `p=none`. That setting is useful for discovery, but it does not enforce.

Enforcement comes from working through the full progression:

- Identify legitimate senders.
- Authenticate them.
- Fix alignment.
- Move to `p=quarantine`.
- Move to `p=reject`.



The DMARC enforcement path: discovery to reject without losing legitimate mail.

In smaller organizations, this can be straightforward. In larger enterprises, the slow part is usually everything before the DNS change: finding every legitimate source sending as the organization.

Marketing platforms, CRMs, helpdesks, billing systems, HR tools, payroll systems, transactional mailers, calendar platforms, multifunction printers, ticketing systems, SaaS products, and departmental tools may all send mail using corporate domains. Some are owned by IT. Many are not.

Use DMARC aggregate reports to discover these senders before enforcing. Each legitimate source needs to be authenticated and aligned, usually by configuring DKIM in the sending platform, keeping SPF under the 10-DNS-lookup limit, sorting out return-path alignment, and coordinating with the team that owns the service.

Go to `reject` too early and you can drop real invoices, password resets, calendar invites, support messages, and customer mail.

Mailing lists and forwarders are the standing exception: they resend mail in ways that break alignment. RFC 9989 advises domains whose users post to mailing lists against `p=reject`, and it requires receivers to treat a failure under bare `p=reject` as quarantine when nothing else corroborates rejection. Plan for that reality: enforce hard on transactional and brand domains, and decide deliberately, with aggregate-report data, how far to push domains that carry heavy list traffic.

For complex estates, stage enforcement. Move from `none` to `quarantine`, monitor the effect, then move to `reject` once legitimate traffic is passing. Stage by domain and subdomain policy. The current DMARC specification, RFC 9989, dropped the old `pct` percentage tag, and receiver support for it was always uneven.

Do not forget subdomains. Threat actors often exploit forgotten or unauthenticated subdomains because the apex domain receives attention and the long tail does not.

BIMI can be useful after enforcement. It gives a visible brand signal in supporting clients and creates an incentive to keep DMARC healthy. BIMI is a brand and trust layer, and DMARC remains the security control beneath it.

Add inbound mail protections as appropriate: anti-phishing policies, impersonation protection, attachment sandboxing, URL rewriting or detonation, user-reporting buttons, and alerting on suspicious forwarding rules. Consider MTA-STS and TLS reporting to improve transport security for mail flows.

If it happens

Work out the mechanism before you react. Pull the DMARC aggregate and forensic reports and check the sending sources and authentication results. True spoofing shows mail failing SPF and DKIM alignment from infrastructure you do not own. If the mail is passing your own signing, treat it as a compromised sender or account and move to **Section 4**, Identity, MFA, and SIM-Swap Resistance.

For confirmed spoofing, contain the abused name without dropping real mail. An unused or dedicated subdomain can go straight to `p=reject`. A live business domain should move to quarantine while you finish verifying every legitimate sender, then on to reject, so you do not lose invoices, password resets, and customer mail mid-incident. Use the report data to identify the sending sources and ask the major mailbox providers to action them. Warn the targeted recipients, finance, customers, and partners, with what to ignore and how to verify a real message. Keep full message headers as evidence, and run the takedown through **Section 16**, The Reactive Takedown Runbook, and the business email compromise playbook in **Section 14**.

OWNERSHIP AND EVIDENCE

OWNER

Email platform owner, security operations, or messaging team.

REVIEW CADENCE

Monthly until enforcement, then quarterly.

EVIDENCE TO RETAIN

DMARC reports, sender inventory, enforcement status, exception list, and subdomain coverage.

KEY METRIC

Percentage of domains and subdomains at DMARC enforcement.

Identity, MFA, and SIM-Swap Resistance

Executive view

Identity is now the front door. Many threat actors get in by logging in: they recover an account, trick a help desk, steal a session, or compromise the phone number used to prove identity.

The business risk is control bypass. An organization may believe MFA is protecting critical systems while the recovery path still depends on a phone number, help desk script, or personal information a threat actor can find.

Leadership should expect high-risk users to have phishing-resistant authentication, hardened recovery paths, and SIM-swap-resistant processes.

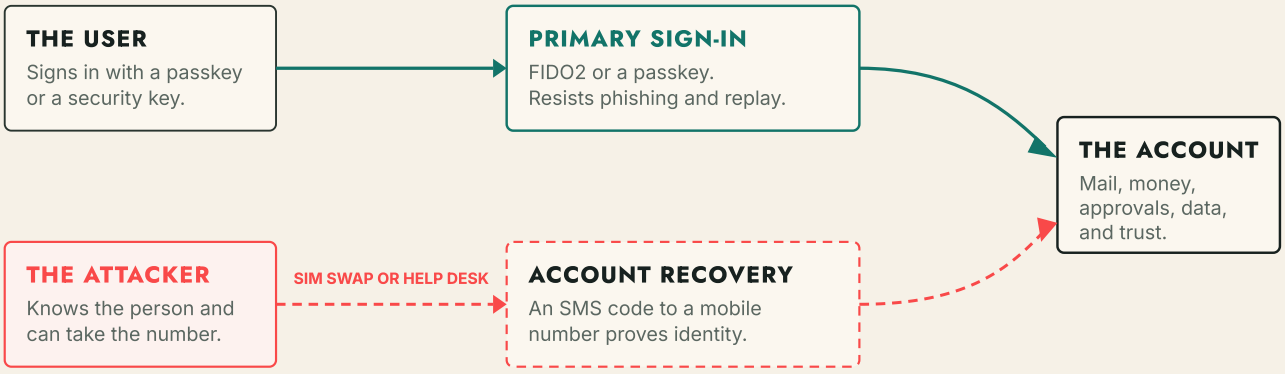
PSYSECURE PRINCIPLE: A recovery path is part of the authentication system. An account is only as strong as the easiest way to recover it, so the password-reset and recovery routes need the same protection as the login itself.

Deeper guidance

MFA everywhere is the baseline, and factor quality matters. SMS codes, voice calls, push approvals, and one-time codes improve on passwords alone while remaining vulnerable to phishing, adversary-in-the-middle proxies, prompt bombing, helpdesk manipulation, token theft, device-code phishing, and SIM swap.

Privileged users, executives, finance staff, domain owners, identity administrators, cloud administrators, developers with production access, and anyone with access to material business systems should use phishing-resistant authentication. Prefer FIDO2 security keys, platform passkeys, or managed passkeys with clear recovery and lifecycle controls. Know whether each passkey is device-bound or synced. A synced passkey inherits the security of the cloud account that syncs it, so that account and its recovery path become part of the system you are defending.

SMS should not be a backup factor for high-risk accounts. A system that uses FIDO2 for login but allows SMS for recovery is still exposed to phone-number compromise. NIST SP 800-63B now classifies phone-based one-time codes as restricted authenticators. Cite it when a platform still treats SMS as the default.



Strong sign-in with weak recovery: the threat actor routes around the front door.

Phone numbers as identity infrastructure

A phone number used for account recovery functions as identity infrastructure.

SIM-swap defense belongs inside the identity program. Threat actors target phone numbers because phone numbers are treated as identity anchors by banks, email providers, password managers, social platforms, cloud services, payroll systems, crypto exchanges, and support desks.

For high-risk personnel, implement these controls:

- Remove SMS and voice call authentication wherever stronger options exist.
- Remove phone numbers from account recovery where possible.
- Use hardware keys or passkeys for primary authentication.
- Require a second phishing-resistant factor or supervised recovery for privileged account resets.
- Add carrier account PINs, number locks, port freezes, and port-out alerts where the carrier supports them.
- Maintain an inventory of business-critical phone numbers and who controls them.
- Treat mobile number changes as security events for executives, finance users, administrators, and public-facing personnel.
- Establish helpdesk scripts that prohibit resetting MFA based only on caller ID, SMS confirmation, personal information, or urgency.
- Monitor for new MFA device registration, MFA method downgrade, password reset, impossible travel, suspicious OAuth grants, new mail-forwarding rules, and changes to payroll or payment details.

For primary business lines, use managed VoIP numbers only when the number-control plane can be administered like an identity system. The value is control. The organization can define who may move, forward, recover, or port a number, and can log and alert on those changes. A carrier number still depends on a support process the organization cannot configure or audit.

VoIP relocates phone-number takeover risk into the account or tenant that controls the number. A VoIP tenant with password-only admin access, weak email recovery, or SMS-backed recovery can be easier to take over than a mobile account protected by a carrier PIN, number lock, and port freeze. A VoIP tenant becomes stronger when administrator access uses phishing-resistant MFA or SSO, least privilege, change alerts, recovery controls, and separation of duties.

Harden the recovery chain behind the VoIP account. The account that controls the number, and the email account that can recover it, should use passkeys or hardware keys and should not fall back to SMS or weak personal mailboxes. Treat number reassignment, call forwarding, port-out requests, and new admin grants as security events. For CPaaS providers, treat API keys that can manipulate numbers as crown-jewel secrets: scoped, vaulted, rotated, IP-restricted where supported, and kept out of code. Set provider port-out locks and account PINs where available.

A phone number remains a weak authentication factor even when the number is well protected. Treat numbers as contact channels. Remove them from account recovery and identity proofing wherever stronger controls exist. A compartmentalized number that is never wired into recovery can be rotated or retired without giving a threat actor a path into other systems.

Do not publish direct mobile numbers for executives, finance staff, IT administrators, HR leaders, legal counsel, or anyone likely to be impersonated. Publish role-based business numbers, call queues, or managed VoIP lines. Keep personal mobile numbers out of public profiles, WHOIS records, press releases, job posts, conference bios, and vendor directories.

Protect session tokens as well as passwords. Modern phishing often steals authenticated sessions rather than credentials. Use conditional access, device compliance, token lifetime controls, sign-in risk policies, and alerts for suspicious OAuth grants or impossible travel.

If it happens

Contain the account, and start with the phone if a number was hijacked. Have the carrier reclaim the line and put a port freeze and SIM lock on the mobile account, then strip SMS and voice as trusted factors, so reset codes and links stop routing to the threat actor. Revoke active sessions and refresh tokens, force a password reset, and re-enroll phishing-resistant authentication from a known-good device. A password reset alone leaves a stolen live session active, so the session and token revocation is the step that locks the threat actor out. Pull their footholds next: remove any MFA methods, app passwords, OAuth grants, and mail rules they added, and check for new delegate, recovery, or forwarding settings.

Work outward from the identity. Map what that account could reach, what it touched during the exposure window, and which systems trusted it, then reset anything it could have authorized. Save the sign-in and audit logs, because they show how far the intruder got. Treat

finance and executive accounts as confirmed breaches: warn the people whose approval that identity can trigger, and hold any payment or payroll change until the account is verified clean.

OWNERSHIP AND EVIDENCE

OWNER

Identity team, help desk owner, and security operations.

EVIDENCE TO RETAIN

MFA method inventory, recovery method review, help desk reset procedure, and high-risk user exception list.

REVIEW CADENCE

Quarterly for high-risk users, with continuous alerting for changes.

KEY METRIC

Percentage of privileged and high-risk users with phishing-resistant MFA and no SMS recovery.

Password Managers and Personal Password Hygiene

Executive view

Password management reduces credential reuse, recovery-path exposure, and personal-account weaknesses that threat actors can use against the organization.

The business risk is spillover. A reused password, breached personal email account, weak family account, or exposed recovery detail can become a corporate compromise path when the person holds authority, access, or public trust.

Leadership should expect corporate password management to be easy to use, strongly protected, and supported beyond the narrow corporate perimeter.

CONTROL GUIDANCE: Perimeter thinking fails when personal accounts control recovery, identity proofing, and executive exposure.

Deeper guidance

Password management is a corporate security control and an OSINT-defense control. Reused passwords, old breach data, weak personal email accounts, exposed family accounts, and compromised recovery paths all come back into the organization through executives, administrators, finance staff, developers, helpdesk workflows, and social engineering.

Do not treat password management as something that stops at the corporate perimeter. Employees use personal email, banking, social media, mobile carriers, cloud storage, shopping accounts, travel accounts, and family devices. Those accounts often contain recovery channels, identity documents, phone numbers, personal details, and information that threat actors can use to compromise or impersonate them at work.

Adopt an enterprise password manager and make it easy to use. Good enterprise password managers support SSO, SCIM or directory provisioning, role-based access, shared vaults, offboarding, audit logs, recovery controls, breach monitoring, passkey support, and policy enforcement. Add one more selection criterion: a sponsored personal or family plan for employees.

Where possible, extend the password manager to employees for personal use. This is one of the most practical security perks an organization can offer, and mature enterprise plans commonly include a sponsored personal or family membership for each employee. That matters because family password hygiene, personal email security, and recovery-account security all influence corporate risk.

Keep work and personal vaults separate. The organization should not have access to personal passwords, and personal accounts should not become shadow storage for corporate credentials. The right model is separation with support: employees get a personal or family password manager benefit, while corporate credentials remain in managed business vaults with enterprise controls.

Require strong master passwords and phishing-resistant MFA for password managers. A password manager concentrates value, so the account protecting it must be treated as high risk. Use hardware keys, passkeys, or strong app-based MFA. Avoid SMS recovery. Review account recovery settings and emergency access paths carefully.

Use shared vaults instead of shared passwords in documents, chats, spreadsheets, browser profiles, or ticket comments. Shared credentials should have owners, rotation expectations, access reviews, and removal on role change or offboarding.

Be careful with vendor selection. Past password-manager incidents reinforce the need to choose vendors with strong architecture, transparent security practices, independent audits, mature incident response, and controls that fit the organization. Security leaders should review encryption design, what metadata is protected or exposed, breach history, recovery model, administrative controls, export controls, logging, and support for passkeys and hardware keys.

Avoid adopting a password manager only for compliance optics. If employees receive a corporate vault but no personal option, they will still reuse passwords at home, store recovery details in personal email, and expose family accounts that threat actors can exploit.

If it happens

Treat every secret in the affected vault as exposed. Revoke the vault's active sessions and trusted devices, then re-secure the account with a new master password and phishing-resistant MFA enrolled from a known-good device. Rotate stored credentials by priority:

- Domain registrar, DNS, and email admin first, then finance, then identity and SSO admin, then anything reused across accounts.
- Force resets on those high-value accounts and check each service for threat actor logins, new MFA methods, app passwords, and recovery or forwarding changes.
- Block known-compromised passwords at reset.

For a breach-corpus hit, force resets on the matched accounts and any that shared the password, and look for successful logins that followed the exposure date. Preserve vault and service audit logs first. **Section 16** covers takedown and reporting, and **Section 14** covers warning the people involved.

OWNERSHIP AND EVIDENCE

OWNER

Identity team, security operations, IT, and HR benefits owner where personal or family plans are sponsored.

REVIEW CADENCE

Quarterly access and policy review, with continuous breach monitoring.

EVIDENCE TO RETAIN

Deployment status, vault access reviews, MFA policy, recovery settings, shared-vault inventory, and offboarding records.

KEY METRIC

Percentage of workforce enrolled, percentage of privileged users protected with phishing-resistant MFA, and number of unmanaged shared credentials found.

OSINT Exposure Reduction

Executive view

Public information becomes attack material. Threat actors use what organizations publish, leak, expose, and allow others to publish about them.

This includes people, vendors, technology, domains, job posts, documents, metadata, phone numbers, email formats, travel, cloud assets, code, and personal details that can help bypass support desks or build convincing social engineering.

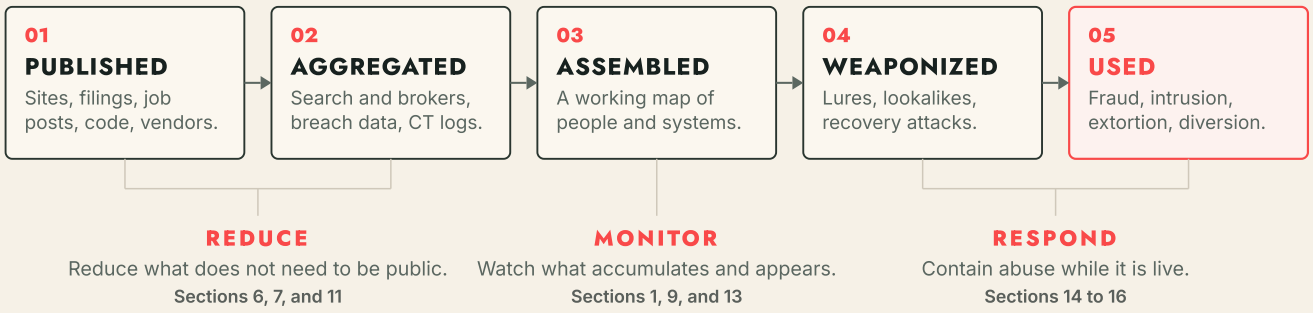
The business risk is unnecessary reconnaissance advantage. The more a threat actor can learn without touching your systems, the easier it is to target your people and processes.

Leadership should expect public exposure to be inventoried, reviewed, reduced, and monitored over time.

PSYSECURE PRINCIPLE: This is where privacy becomes a security control. Each detail kept out of public view, personal or corporate, is one less fact a threat actor can use to impersonate, target, or deceive your people.

Deeper guidance

Threat actors build better lures when they can see more. They use public information to identify who approves payments, which vendors you use, when executives travel, what technology stack you run, who recently joined, which projects are active, what your email format is, which subsidiaries exist, which cloud services are exposed, and which personal details can help bypass support desks.



How public exposure becomes an attack path, and where the controls in this guide cut it.

Start with a public-footprint inventory. Include corporate websites, subdomains, microsites, job postings, social media, executive bios, press releases, PDFs, GitHub repositories, package registries, mobile apps, app store listings, cloud assets, exposed APIs, vendor case studies, partner directories, conference agendas, podcasts, webinars, WHOIS and RDAP records, CT logs, breach corpora, paste sites, and data broker listings.

Classify exposed information by abuse value. The most useful information to threat actors includes:

- Email formats and direct contact details.
- Executive and finance-team names.
- Personal mobile numbers.
- Travel patterns and event attendance.
- Calendar free-busy detail, scheduling links, and out-of-office replies.
- Vendor relationships.
- Technology stack details.
- VPN, SSO, mail, remote access, and admin portals.
- Internal document metadata.
- Org charts and reporting lines.
- Payroll, HR, legal, finance, and procurement workflows.
- Personal details used for support-desk verification.
- Photos of badges, offices, desks, screens, vehicles, or access controls.
- Public code, secrets, tokens, `.env` files, and configuration examples.

Reduce what does not need to be public. Replace personal addresses with role-based addresses. Remove direct mobile numbers. Strip metadata from documents. Review executive biographies for unnecessary family, travel, school, hometown, and assistant details. Remove stale team pages. Limit job posts that disclose exact security tooling, cloud architecture, or internal project names. Ask vendors to remove unnecessary case-study details. Use privacy-protected domain registration where appropriate. Keep sensitive repositories private. Remove exposed keys and rotate them immediately.

Review public job posts for unnecessary disclosure of security tools, cloud providers, internal project names, incident-response vendors, and architecture details. Job posts are one of the easiest ways to fingerprint an organization's stack.

This work should not be a one-time cleanup. Public exposure drifts constantly. Marketing launches new pages, HR posts new jobs, vendors publish customer logos, developers create repositories, executives speak at events, and employees update profiles. Build a recurring OSINT review cadence.

If it happens

Triage by abuse value and work the highest first. Anything that is a live secret stays valid until you change it, and removal does not undo the exposure once the material is indexed, so rotation comes before takedown.

- Rotate exposed keys, tokens, and credentials, then check logs for use during the exposure window.
- Ask the host to take the content down, and submit removal requests to Google Search and Bing.
- File data-broker and people-search opt-outs for each named person.
- Warn the people the material exposes so they recognize the matching lure, and watch for it.
- Log every removal request, the provider response, and what is still outstanding.

If the material already drove an impersonation campaign, run **Section 16**, The Reactive Takedown Runbook, and brief the people through **Section 14**.

OWNERSHIP AND EVIDENCE

OWNER

Security, privacy, communications, legal, and executive office jointly.

REVIEW CADENCE

Quarterly, plus review before major announcements, executive events, and vendor case studies.

EVIDENCE TO RETAIN

Exposure inventory, removal requests, vendor publication approvals, data broker review, and executive exposure review.

KEY METRIC

Number of high-value exposures remediated or accepted with rationale.

Executive and High-Risk-Person Protection

Executive view

Executives, founders, board members, finance leaders, legal counsel, HR leaders, domain owners, and senior administrators carry risk beyond their job titles. Threat actors target their authority, their personal footprint, and the systems that trust them.

The business risk is that personal exposure becomes organizational compromise. A personal email account, public phone number, fake profile, weak recovery path, or convincing voice clone can become the first step in fraud, extortion, credential theft, payment diversion, or reputational harm.

Leadership should expect high-risk people to receive a different security model than the general workforce.

PSYSECURE PRINCIPLE: For high-risk personnel, corporate account security and public exposure have to be reviewed together: what can be used to impersonate, coerce, deceive, or recover access through them?

Deeper guidance

The protection model for high-risk people reaches accounts the organization does not own. Corporate controls stop at the corporate identity, while the pivot points sit in personal email, phone numbers, social profiles, and the household, so the program needs the person's consent and participation to work.

Protect corporate and personal email for high-risk individuals. Personal email often controls recovery for banking, travel, cloud accounts, social media, and consumer services. Encourage high-risk users to enroll in advanced protection programs where available, use hardware security keys or passkeys, remove SMS recovery, and review account recovery options.

Treat the household as attack surface. Once the executive's own accounts are hardened, threat actors pivot to a spouse's email, a child's gaming or social accounts, or a shared family cloud account, because those hold the same photos, locations, calendars, and recovery channels behind weaker protection. Shared family cloud accounts deserve specific attention: they often sit in the recovery chain for devices, photo libraries, and app stores. Extend the sponsored password manager benefit from Section 5 to the family, move family accounts to unique passwords and phishing-resistant MFA where supported, and cover home-network basics: current router firmware, changed default admin credentials, and a guest or separate network for IoT devices.

Harden phones and messaging. Require strong device passcodes, current operating systems, encrypted backups, secure messaging for sensitive conversations, and mobile threat controls where appropriate. Avoid using personal mobile numbers as business identity anchors. Use managed VoIP for public business communications only where administrator access, logging, recovery, and change alerts are owned, and where the controlling account has no weak SMS or email recovery path. Reserve mobile numbers for limited internal use.

Plan around travel and public appearances. Conference agendas, speaking slots, flight patterns, and event photos tell threat actors where a person will be and when their attention is split, and that timing feeds both physical approaches and well-timed fraud. Brief high-risk people before visible events, post about locations after leaving them, strip location metadata from what does get published, and treat the itinerary itself as exposure to manage.

Calendar exposure deserves the same review. Free-busy visibility outside the organization, public scheduling links, and out-of-office replies that name destinations and dates hand threat actors the timing for impersonation: a wire request sent while the CFO is mid-flight lands because the threat actor knew about the flight. Restrict external calendar sharing, keep scheduling links generic, and write out-of-office replies that give a contact path without an itinerary.

Protect against impersonation. Monitor social platforms, messaging platforms, domain registrations, and search results for fake executive profiles, fake recruiter accounts, fake support accounts, fake investment accounts, and fake payment instructions.

Treat data-broker suppression as a subscription, because the data repopulates. Brokers reacquire records from fresh public sources within months of a successful opt-out, so a one-time cleanup quietly expires. Run suppression for high-risk people on a cadence, through a removal service or an owned internal process, and measure re-appearance rather than requests filed.

Create verification protocols for sensitive requests. Payment changes, bank detail changes, urgent wire approvals, gift card requests, payroll changes, legal instructions, access requests, and confidential document sharing should require out-of-band verification using trusted channels. The verification channel must be one that was set up in advance. A phone number or address supplied inside the suspicious request itself never qualifies.

Deepfake and voice-clone risk makes this more important. A familiar voice or face should not be enough to authorize money movement, credential reset, legal action, or sensitive disclosure. Use call-back procedures, shared verification phrases for emergency contexts, dual approval, and transaction holds for unusual requests.

Executive Exposure Advisory naturally belongs here: identify what threat actors can learn about high-risk people, reduce what they can use, and build repeatable protection around public exposure, identity recovery, impersonation, and verification workflows.

If it happens

Stop the money first. Place an immediate hold on any payment, payroll, or bank-detail change tied to the request, and verify it out-of-band with the real person through the channel agreed in advance. Confirmation comes only through that pre-set channel, no matter how convincing the voice, the video, or the tone of the request.

Then contain the spread. Report the impersonating profile, clone, or content through the routes in **Section 16**, preserving profiles, messages, headers, and transaction details as you go. Warn finance, HR, executive assistants, and anyone else the threat actor is likely to message next, and brief them on the live pretext per **Section 14**.

For doxxing, start removals, bring in legal, and weigh physical-safety steps for the individual and their family. Keep every artifact: it drives both the takedown and any law-enforcement referral.

OWNERSHIP AND EVIDENCE

OWNER

Executive sponsor, CISO, executive office, identity team, legal, and executive protection where applicable.

EVIDENCE TO RETAIN

High-risk person inventory, exposure review, account protection status, verification protocols, data-broker suppression status, and impersonation reports.

REVIEW CADENCE

Quarterly for high-risk personnel, with event-based reviews before major public exposure.

KEY METRIC

Percentage of high-risk personnel reviewed for account protection, phone-number exposure, recovery paths, and impersonation risk.

Subdomain Takeover and Dangling DNS

Executive view

Subdomains often outlive the systems they point to. When a forgotten DNS record still references a third-party service, a threat actor may be able to claim the abandoned resource and inherit a trusted branded name.

The business risk is quiet trust transfer. The organization may still own the domain, but the branded subdomain can serve threat-actor-controlled content, capture credentials, host malware, or support phishing.

Leadership should expect DNS cleanup to be tied to asset lifecycle, vendor offboarding, product retirement, and cloud teardown.

CONTROL GUIDANCE: DNS records are assets. If nobody owns their lifecycle, abandoned names become threat actor opportunities.

Deeper guidance

Dangling DNS remains a quiet and common foothold. A team points `status.example.com` at a cloud service, tears down the cloud resource later, and forgets the DNS record. The name now points at a resource that may be claimable by someone else. A threat actor claims it and inherits your branded subdomain.

Enumerate DNS records continuously. Flag CNAME, ALIAS, and other records pointing at third-party platforms. Verify that each target still resolves to an asset you control. Tie DNS cleanup to cloud teardown, vendor offboarding, marketing campaign shutdown, and product retirement.

Monitor CT logs for unexpected certificates on your subdomains. A certificate appearing for a subdomain you did not provision may indicate a takeover, shadow IT, or vendor drift.

If it happens

Severing the takeover is one DNS change. Have the DNS owner remove or repoint the offending record so the branded subdomain stops resolving to the threat actor's resource, then reclaim or properly decommission the third-party service the record pointed at. Check CT logs for any certificate issued for that subdomain, and report and take down live abuse through the channels in Section 16, The Reactive Takedown Runbook.

Then close what trusted the name. Work out what scoped trust to that subdomain: session cookies set on the parent domain, CORS allowlists, OAuth redirect URIs, and SSO callbacks. Revoke or tighten each one. Preserve the DNS history, certificate records, and any captured content as evidence, and run customer or staff notification through **Section 14** when phishing reached real people.

OWNERSHIP AND EVIDENCE

OWNER

DNS owner, cloud infrastructure team, and security operations.

REVIEW CADENCE

Continuous monitoring with monthly cleanup review.

EVIDENCE TO RETAIN

DNS inventory, third-party target validation, decommission records, CT alerts, and remediation tickets.

KEY METRIC

Number of dangling or unowned DNS records found and remediated.

External Attack Surface and Exposure

Executive view

Organizations cannot protect assets they do not know they own. Internet-facing systems, exposed admin portals, forgotten cloud resources, SaaS tenants, and old VPN appliances create risk precisely because they fall outside the clean inventory.

The business risk is unmanaged exposure. A known-exploited vulnerability on an internet-facing system can matter more than a theoretical critical issue buried deep inside the environment.

Leadership should expect asset inventory, exposure discovery, and vulnerability prioritization to run as one connected workflow.

PSYSECURE PRINCIPLE: The asset you forgot you owned is the one a threat actor finds first. The old VPN appliance, the staging server, the cloud account no one closed: each stays exposed precisely because no one is still watching it.

Deeper guidance

Maintain an inventory of internet-facing systems, domains, certificates, cloud accounts, SaaS tenants, APIs, mobile apps, exposed storage, VPN portals, remote access systems, mail gateways, identity providers, and administrative panels.

Run self-recon the way a threat actor would. Use search engines, Shodan, Censys, CT logs, passive DNS, GitHub, package registries, breach data, app stores, cloud asset discovery, and SaaS inventories. Look for exposed admin panels, RDP, databases, staging systems, forgotten dev hosts, default pages, debug endpoints, old VPN appliances, and systems running technology with known exploited vulnerabilities.

Patch known-exploited vulnerabilities first. Raw CVSS is not enough. A medium-scored flaw under active exploitation on an exposed system often outranks a higher-scored vulnerability sitting on an isolated host. Use CISA KEV as the first priority input. For the long tail outside KEV, use the Exploit Prediction Scoring System (EPSS) to surface vulnerabilities more likely to be exploited, then combine those signals with asset criticality, exposure, business impact, and compensating controls.

For systems that cannot be patched quickly, especially OT, medical, embedded, or legacy platforms, document compensating controls: isolation, access control, virtual patching, detection, vendor mitigation, service shutdown, or replacement timeline.

Publish a `security.txt` file under `/.well-known/` on your primary domains (RFC 9116). Outside researchers often see an exposure first, and a published security contact shortens the path from their discovery to your fix.

If it happens

Pull the host off the network or apply a virtual patch at the gateway to stop the active exploitation. Treat every credential, API key, certificate, and token on that system as exposed, and rotate them: service accounts, cloud keys, and anything the host could authenticate with.

Then hunt outward from the foothold. Assume the threat actor moved, and look for persistence, new accounts, and lateral movement into systems the host could reach. Image the disk and pull the logs before you wipe anything, because rebuilding destroys the record of how far the threat actor reached and what you owe legal and your insurer. Only then patch the known-exploited vulnerability or rebuild from a known-good image and return the system to service. Meet the incident-reporting obligations that apply to you, from regulators to your cyber insurer to customer contracts, and run the ransomware or other relevant playbook in **Section 14** and the takedown runbook in **Section 16** where they apply.

OWNERSHIP AND EVIDENCE

OWNER

Vulnerability management, infrastructure, cloud platform owners, and security operations.

REVIEW CADENCE

Continuous discovery with weekly triage for internet-facing risk.

EVIDENCE TO RETAIN

External asset inventory, scan records, KEV and EPSS triage, exception records, and compensating-control documentation.

KEY METRIC

Time to remediate or mitigate known-exploited and high-likelihood vulnerabilities on internet-facing systems.

Browser Security and Web Exposure

Executive view

The browser is now a primary enterprise workspace. Email, SaaS, identity, file sharing, admin consoles, customer systems, AI tools, and payment workflows all pass through it.

The business risk is session and data compromise at the point where people work. A weak browser posture turns phishing, malicious extensions, session theft, data leakage, shadow SaaS, and unsafe AI-tool use into everyday operating risk.

Leadership should expect browsers to be patched, governed, extension-limited, privacy-protective, and separated by risk.

CONTROL GUIDANCE: The browser is part of identity security. It holds your people's live, logged-in sessions, so a stolen session or a malicious extension can hand a threat actor the account without ever needing the password or MFA.

Deeper guidance

Manage browsers as part of the security baseline. Enforce automatic updates, safe browsing protections, password manager policy, download controls, certificate warnings, DNS-over-HTTPS policy, extension governance, profile separation, and restrictions on syncing corporate data into personal accounts.

Treat extensions as privileged software. Browser extensions can often read and change page content, capture data, inject scripts, and follow users across sites. Maintain an allowlist for approved extensions, block unknown extensions by default where possible, and review extension permissions, ownership, update history, and business need. Remove abandoned or unnecessary extensions.

Block avoidable web tracking and malvertising. A privacy-protective browser configuration reduces both surveillance and attack surface. Choose browsers on capability: built-in or policy-enforced tracker and fingerprinting protection, ad and malvertising blocking, enterprise manageability, and extension governance. Blocking that ships in the browser or arrives by policy survives better than blocking that depends on each user installing and maintaining an extension. In Chrome or Edge estates, use enterprise policy to restrict extensions and apply safe browsing, site isolation, download, and data-loss controls.

Separate work and personal browsing. Corporate identity, SaaS sessions, admin consoles, and sensitive documents should not share the same browser profile as personal mail, shopping, social media, crypto, or unmanaged extensions. For privileged users, consider dedicated

browser profiles, dedicated admin workstations, or remote browser isolation for high-risk workflows.

Monitor for browser-level signals: suspicious extensions, new OAuth grants, impossible travel followed by SaaS access, session-token theft indicators, unusual downloads, credential entry into lookalike domains, and corporate data pasted into unsanctioned AI or file-sharing services.

Success means browsing is governable: patched, policy-controlled, extension-limited, privacy-protective, and separated by risk.

If it happens

Document the extension before you remove it. Capture its ID, version, and permission set and pull the relevant browser and proxy logs, then block it across all managed browsers so the artifact survives the purge. Revoke active sessions, refresh tokens, and OAuth grants for affected users and force re-authentication. Assume the threat actor holds a live session, so a password reset alone leaves them inside. Pivot to **Section 4** for the identity clean-up: mail rules, delegate and forwarding settings, and any MFA methods they added.

Now scope it. Inventory what the extension could read or change, and check browser and proxy logs for data sent to its endpoints during the exposure window. For broader takedown and notification steps, follow the Reactive Takedown Runbook in **Section 16**.

OWNERSHIP AND EVIDENCE

OWNER

Endpoint management, IT, security operations, and identity team.

REVIEW CADENCE

Monthly policy and extension review, with continuous update compliance monitoring.

EVIDENCE TO RETAIN

Browser policy baselines, extension allowlist, exception list, update compliance, and browser security alerts.

KEY METRIC

Percentage of managed browsers compliant with update, extension, and profile-separation policy.

Data, Credential, and Secret Exposure

Executive view

Credentials, secrets, code, documents, SaaS shares, AI prompts, and public storage all contribute to the public-information attack surface.

The business risk is that sensitive material can become useful before the organization notices it was exposed. Threat actors test leaked credentials quickly, reuse exposed secrets, mine documents for metadata, and turn public links into long-lived access paths.

Leadership should expect credential monitoring, secret scanning, cloud-storage review, metadata hygiene, SaaS sharing governance, and AI-tool rules to operate as one exposure program.

PSYSECURE PRINCIPLE: Threat actors use what the organization assumes is harmless.

Deeper guidance

The OSINT-defense surface includes credentials, secrets, code, documents, and storage.

Monitor breach corpora for corporate email addresses and exposed credentials. Staff reuse passwords despite policy. When a third party is breached, those credentials are tested against your systems quickly. Force resets when corporate credentials appear in credible breach data, and block known-compromised passwords at creation and reset.

Scan public code hosting for secrets, API keys, cloud credentials, tokens, private keys, webhooks, connection strings, and `.env` files. Add pre-commit scanning and CI scanning so secrets are caught before publication. When a secret is exposed, rotate it. Deleting the commit is not enough.

Audit public cloud storage. Public buckets, blobs, snapshots, container registries, and shared links routinely leak data. Inventory public exposure and require business justification for anything intentionally public.

Strip document metadata before public release. PDFs, spreadsheets, presentations, and images may expose author names, usernames, internal paths, software versions, GPS data, printer names, comments, tracked changes, hidden sheets, and internal document history.

Control SaaS sharing. Public links, external guest access, unmanaged OAuth apps, abandoned workspaces, shared drives, and contractor accounts can become long-lived exposure points. Review who has external access and what can be indexed or downloaded.

Control what employees paste into public AI tools. Treat prompts, uploaded documents, screenshots, logs, customer data, source code, and credentials as possible data exposure. Provide approved AI tools and clear rules rather than pretending employees will not use them.

If it happens

Rotate or revoke the secret immediately. Deleting the commit, file, or share does not undo the exposure, so assume the credential was already collected and used. Before you rotate a shared or service credential, list the systems that depend on it and update them together, so the rotation does not cause an outage that tempts a partial reset. Then trace what the credential could reach: pull the access and audit logs of every system it could authenticate to, review them for use across the exposure window, and reset anything it could have authorized.

Lock down the exposed buckets, blobs, snapshots, registries, and shared links, and confirm none of them stayed reachable to anonymous or unintended parties. If customer or regulated data was reachable, start breach assessment and notification with legal. Run this against the public secret exposure and cloud storage exposure playbooks in **Section 14**.

OWNERSHIP AND EVIDENCE

OWNER

Security operations, data governance, cloud platform owners, SaaS application owners, and engineering.

REVIEW CADENCE

Continuous scanning with monthly exposure review.

EVIDENCE TO RETAIN

Credential exposure alerts, secret scanning results, rotation records, cloud storage inventory, SaaS sharing review, and AI-tool policy.

KEY METRIC

Time from exposure detection to credential reset, secret rotation, or public-access removal.

Backup and Resilience

Executive view

Backups turn a ransomware catastrophe into a recoverable incident only if they are designed, protected, and tested correctly.

The business risk is false confidence. A backup that can be encrypted by the same threat actor, administered through the same compromised identity, or never restored in practice may not exist when the business needs it.

Leadership should expect immutability, separation, restore testing, and measured recovery outcomes.

CONTROL GUIDANCE: A backup you have never restored is a hypothesis.

Deeper guidance

Use 3-2-1 with immutability: three copies, two different storage types or locations, one off-site, and at least one copy that threat actors cannot encrypt or delete. Immutable or offline backups matter because ransomware operators target backup systems early.

Test restores. Schedule restore drills, measure recovery time, confirm data integrity, and include identity systems, DNS, cloud control planes, SaaS data, endpoint images, business applications, and critical file stores.

Protect backup administration separately. Backup consoles should not share the same identity, network, or administrative exposure as the systems they protect. Assume threat actors already know which backup platform you run, because job posts and vendor case studies usually say so, and protect the consoles accordingly.

If it happens

Recovery waits until you have contained the threat actor. Isolate the affected systems, lock the backup consoles to a separate identity, and pull their active sessions, so your copies cannot be reached or re-encrypted.

Then confirm you actually hold a clean copy. Locate an immutable or offline backup, validate its integrity, and check it predates the intrusion before you trust it. Restore into a clean, isolated recovery environment rather than back onto the compromised network. Bring systems up in dependency order: identity, DNS, and cloud control planes, then the applications that rely on them. Validate each control plane for persistence before you trust it, because

hidden admin or service accounts, federation and SSO trust changes, rogue OAuth or app registrations, and forwarding rules all survive a restore. Rebuild compromised hosts from known-good images. Cleaning in place leaves footholds.

Bring in incident response, legal, and your cyber insurer at the start, and keep logs as evidence. Do not pay reflexively. A ransom decision belongs with legal, your insurer, and law enforcement, because payment can carry sanctions and regulatory exposure and still does not guarantee recovery. Run this alongside the ransomware playbook in **Section 14**.

OWNERSHIP AND EVIDENCE

OWNER

Infrastructure, backup platform owner, business application owners, and security operations.

REVIEW CADENCE

Quarterly restore testing, with continuous backup job monitoring.

EVIDENCE TO RETAIN

Backup architecture, immutability settings, restore-test results, recovery-time measurements, and backup administrator access review.

KEY METRIC

Percentage of critical services with successful restore test inside recovery objectives.

Logging and Detection Basics

Executive view

Detection depends on the logs the organization actually keeps. Many incidents become harder to investigate because identity, SaaS, email, DNS, registrar, cloud, or endpoint logs aged out before anyone knew a compromise had occurred.

The business risk is delayed truth. Without the right logs and high-signal alerts, the organization may not know what changed, who accessed what, how far the incident went, or whether recovery is complete.

Leadership should expect logging coverage for the systems that carry identity, money movement, data access, domain control, and administrative authority.

CONTROL GUIDANCE: You can start watching high-signal events well before you have a mature SOC. What that takes is ownership, coverage, and a clear response path.

Deeper guidance

Centralize the logs that matter: identity provider, endpoint, cloud control plane, SaaS administration, email, DNS, registrar, VPN, privileged access, EDR, source control, CI/CD, and critical applications.

Retain logs long enough to investigate slow intrusions. Many breaches become uninvestigable because logs aged out before the organization knew anything happened.

Alert on high-signal events:

- New MFA device on a privileged or executive account.
- MFA method downgrade or SMS recovery added.
- Password reset for a high-risk user.
- New mail-forwarding or inbox-hiding rule.
- Suspicious OAuth consent grant.
- Impossible travel or anomalous login.
- New administrator role assignment.
- DNS, registrar, or nameserver change.
- New certificate for an unexpected domain or subdomain.
- Mass download from SaaS or file storage.
- Public sharing enabled on sensitive data.
- New external guest added to sensitive workspaces.

- Payment, payroll, or bank detail change.
- Login from anonymizing infrastructure.
- Successful authentication after credential exposure.
- Suspicious browser extension installed or enabled.
- Public AI tool use involving sensitive corporate data.

Include administrative actions in SaaS platforms alongside cloud and identity systems. Many incidents now happen entirely inside SaaS: file sharing, OAuth grants, mailbox rules, exports, external guests, API tokens, and permission changes.

Most of these signals are the fingerprints of recovery-path and exposure abuse. The alert list is how you catch the account takeovers of **Section 4** and the executive targeting of **Section 7** while they are still in progress.

If it happens

Preserve the logs before they age out. Export from the identity provider, email, endpoint and EDR, DNS, registrar, cloud control plane, SaaS administration, VPN, and privileged access, and store the exports off the systems under suspicion. Set retention holds where the platform allows it.

Build a timeline next. Anchor it on the high-signal events: a new MFA device, a mail-forwarding or inbox-hiding rule, an OAuth consent grant, impossible travel, an admin role assignment, a payment or bank-detail change. Those markers fix when access began and how long the intruder held it.

Then map what is in scope. List the accounts, mailboxes, and systems that identity could reach, and hand a clean evidence package to incident response. Run containment per **Section 16**, and escalate through the relevant **Section 14** playbook.

OWNERSHIP AND EVIDENCE

OWNER

Security operations, IT, cloud platform owners, identity team, and SaaS application owners.

REVIEW CADENCE

Monthly coverage review and continuous alert monitoring.

EVIDENCE TO RETAIN

Log source inventory, retention settings, alert rules, response procedures, and incident review records.

KEY METRIC

Percentage of high-value systems sending required logs with sufficient retention.

Human Layer and Incident Readiness

Executive view

Your people are usually the first to notice an attack, often before any security tool does. A workforce that reports suspicious activity quickly gives security teams a chance to contain social engineering before it becomes a business crisis.

The business risk is procedural weakness. Modern social engineering crosses email, messaging, phone, video, collaboration tools, supplier accounts, and AI-generated media. If approval paths are informal, threat actors will exploit urgency and authority.

Leadership should expect reporting-friendly training, verification protocols, realistic playbooks, and tabletop exercises that test decisions before the real event.

PSYSECURE PRINCIPLE: A verification channel only counts if it was established before the suspicious request arrived.

Deeper guidance

Training should make reporting easy and safe. Phishing simulations that optimize for humiliation or click-rate punishment suppress the behavior you need most: fast reporting.

Measure reporting speed, reporting rate, and whether reports arrive before damage. A user who clicks and reports inside a minute does more for containment than one who never clicks and never reports.

Prepare for modern social engineering. Email is only one channel. Threat actors use SMS, WhatsApp, Signal, Teams, Slack, LinkedIn, phone calls, QR codes, shared documents, fake calendar invites, fake browser updates, device-code phishing, AI-generated audio, fake recruiters, fake vendors, and compromised supplier accounts.

Create playbooks for the predictable cases:

- Business email compromise.
- Payroll diversion.
- Vendor bank-detail change.
- Executive impersonation.
- SIM swap.
- Domain impersonation.
- Ransomware.
- Stolen session token.

- Compromised OAuth application.
- Public secret exposure.
- Cloud storage exposure.
- Dangling subdomain takeover.
- Lost or stolen executive device.
- Browser extension compromise.
- Sensitive data pasted into an unsanctioned AI tool.

Run tabletop exercises against realistic scenarios. The value comes from exercising decisions, escalation paths, authority, communications, legal involvement, customer impact, and recovery actions before the real event.

If it happens

Thank the person who reported it and keep blame out of the conversation. Fast reporting is what limits the damage, and the next report depends on this one going well.

Contain based on what they did:

- Credentials entered: revoke active sessions and refresh tokens, force a password reset, and re-enroll MFA from a known-good device.
- Something installed: isolate the device from the network and hand it to incident response.
- Money moved: tell finance to freeze and recall the transaction, then notify the bank and fraud team.

Then open the matching playbook from the list above, and run the takedown steps in **Section 16**, The Reactive Takedown Runbook. Assume the same campaign reached others. Search mail and messaging for the lure, and tell affected teams what it looks like and how to report it.

OWNERSHIP AND EVIDENCE

OWNER

Security awareness, incident response, legal, communications, finance, HR, and executive office.

REVIEW CADENCE

Quarterly tabletop or scenario review, with continuous reporting monitoring.

EVIDENCE TO RETAIN

Training records, reporting metrics, playbooks, tabletop findings, and verification procedures.

KEY METRIC

Median suspicious-message reporting time and percentage of high-risk workflows with defined verification protocol.

Vendor and Third-Party OSINT Risk

Executive view

Your public footprint includes what other people publish about you.

Vendors, agencies, law firms, recruiters, MSPs, MSSPs, integration partners, resellers, event organizers, and customers may reveal information that helps threat actors target your organization. Case studies, testimonials, screenshots, job ads, support articles, conference talks, and partner pages can expose tooling, architecture, contacts, timelines, workflows, and internal assumptions.

The business risk is loss of control over your own exposure.

Leadership should expect vendor publication rights, case studies, screenshots, logos, and architecture references to be governed.

PSYSECURE PRINCIPLE: Vendor-published information is still your exposure.

Deeper guidance

Maintain a third-party exposure register. Track which vendors are allowed to use your name, logo, case-study details, architecture diagrams, personnel names, screenshots, or implementation details. Require approval before publication. Review public vendor references periodically.

Add third-party OSINT review to vendor onboarding and renewal. Ask two questions: “Can this vendor protect our data?” and “What is this vendor allowed to publish about us?”

Third-party compromise is also an impersonation problem. Threat actors who compromise a supplier can send believable payment changes, document links, contract updates, or support requests from real infrastructure. Sensitive vendor requests should use verification paths that do not depend solely on the email thread.

If it happens

Start with the live request. Verify any in-flight payment change, bank-detail update, or document link out-of-band through a path that does not touch the email thread: call a known contact on a number you already hold, and hold the payment until it clears that check.

Then work the exposure. Find out what data the vendor held and what was reached, and ask them to remove material that exposes your tooling, architecture, or people. Rotate any shared credentials, API tokens, or access the relationship used. Warn the internal owners who deal

with that supplier to expect impersonation, and tell them which requests to distrust. Record the exposure and the removal request in the third-party exposure register. If money moved or a spoofed asset is live, run the **Section 16** takedown order and brief the people through **Section 14**.

OWNERSHIP AND EVIDENCE

OWNER

Vendor risk, legal, procurement, communications, and security.

EVIDENCE TO RETAIN

Publication approvals, vendor exposure register, case-study review records, and removal requests.

REVIEW CADENCE

At onboarding, renewal, and before public case studies.

KEY METRIC

Percentage of critical vendors with publication restrictions and exposure review.

The Reactive Takedown Runbook

Executive view

When a lookalike domain, fake profile, spoofed page, or impersonation campaign is already live, speed matters. The organization needs to interrupt victim traffic, remove content, preserve evidence, and warn affected people before the campaign causes more harm.

The business risk is response delay. Abuse reports, browser warnings, registrar actions, platform reports, legal routes, customer alerts, and banking notifications may all be needed at once.

Leadership should expect a practical takedown process with pre-approved owners, evidence templates, provider contacts, and customer communications paths.

CONTROL GUIDANCE: The fastest takedown starts before the crisis, with the evidence package and owner list already prepared.

Deeper guidance

Takedown work runs in parallel because every channel has its own clock. Browser warnings can land within hours, hosting and registrar actions take hours to days, platform responses vary widely, and legal routes run on weeks. Waiting on any single channel hands the campaign more victims.

First response order

ACT IN PARALLEL

01	**REPORT THE URL FIRST**	Browser and platform protections interrupt victim traffic before any takedown completes.
02	**FILE ABUSE WITH HOST AND REGISTRAR**	They are usually different parties. File with both, plus the CDN, mail, and social platforms.
03	**LEAD WITH EVIDENCE**	URLs, timestamps, WHOIS or RDAP, DNS records, certificate details, headers, screenshots.
04	**USE TRADEMARK ROUTES WHERE THEY FIT**	UDRP and URS recover or suspend domains on legal timelines, after the live campaign is contained.
05	**WARN THE PEOPLE AT RISK**	Name the legitimate channels, say what to ignore, and give people a reporting path.

The first response order runs as parallel workstreams, with evidence attached to every report.

Report the URL to browser and platform protection ecosystems. Browser warnings can interrupt victim traffic even before the domain is suspended.

File abuse reports with the hosting provider, CDN, registrar, DNS provider, email provider, social platform, payment processor, and any marketplace involved. The content host and registrar are usually different parties, so file both.

Lead with evidence. Include screenshots, URLs, timestamps, WHOIS or RDAP data, DNS records, certificate details, hosting details, side-by-side comparison with the legitimate site, message headers, payment details, customer reports, and trademark information where available.

Use trademark routes when appropriate. UDRP and URS are useful for asset recovery or suspension, but they are not emergency response tools. They operate on legal timelines, while phishing campaigns often operate on hours.

Warn customers and staff quickly when harm is likely. Publish a clear alert, tell people what not to do, identify the legitimate channels, and provide a reporting path. If money moved, notify banks, payment processors, fraud teams, and relevant reporting bodies.

Takedown and reporting links

Browser and security ecosystem reporting:

- Google Safe Browsing phishing report: https://safebrowsing.google.com/safebrowsing/report_phish/
- Google Safe Browsing malware or unwanted software review: https://safebrowsing.google.com/safebrowsing/report_error/
- Microsoft Defender SmartScreen unsafe site report: https://www.microsoft.com/en-us/wdsi/support/report-unsafe-site-guest
- APWG phishing report by email: reportphishing@apwg.org
- VirusTotal URL submission: https://www.virustotal.com/gui/home/url
- URLhaus malware URL reporting: https://urlhaus.abuse.ch/

Cloud, CDN, registrar, and hosting abuse:

- Cloudflare abuse report: https://abuse.cloudflare.com/
- Cloudflare phishing report: https://abuse.cloudflare.com/phishing
- AWS abuse report: https://support.aws.amazon.com/#/contacts/report-abuse
- Google Cloud abuse report: https://support.google.com/code/contact/cloud_platform_report
- Namecheap abuse guidance: https://www.namecheap.com/support/knowledgebase/article.aspx/9196/5/how-and-where-can-i-file-abuse-complaints/
- GoDaddy abuse report: https://supportcenter.godaddy.com/AbuseReport
- ICANN registrar lookup: https://lookup.icann.org/

- IANA registrar list: https://www.iana.org/assignments/registrar-ids/registrar-ids.xhtml

Law enforcement and fraud reporting:

- FBI IC3, United States: https://www.ic3.gov/
- Report Fraud, England, Wales, and Northern Ireland: https://www.reportfraud.police.uk/
- Canadian Anti-Fraud Centre: https://antifraudcentre-centreantifraude.ca/report-signalez-eng.htm
- Australian Cyber Security Centre ReportCyber: https://www.cyber.gov.au/report-and-recover
- Europol cybercrime reporting country directory: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

Social platform impersonation reporting:

- LinkedIn fake profile report: https://www.linkedin.com/help/linkedin/answer/a1338436
- X impersonation report: https://help.x.com/en/forms/authenticity/impersonation
- Facebook impersonation report, may require login: https://www.facebook.com/help/contact/295309487309948
- Instagram impersonation report, may require login: https://help.instagram.com/contact/636276399721841
- TikTok report impersonation guidance: https://support.tiktok.com/en/safety-hc/report-a-problem/report-an-impersonation-account
- YouTube privacy and impersonation complaints: https://support.google.com/youtube/answer/2801947

Search and content removal:

- Google Search content removal: https://support.google.com/websearch/troubleshooter/3111061
- Bing content removal: https://www.bing.com/webmasters/tools/content-removal

Maintain an internal version of this list with account-specific details for your registrar, DNS provider, CDN, cloud providers, email provider, payment processor, legal counsel, cyber insurer, takedown vendor, and communications owner. The public links are useful, but the fastest response usually comes from knowing exactly which provider owns the infrastructure and having the evidence package ready.

OWNERSHIP AND EVIDENCE

OWNER

Security operations, legal, communications, fraud team, customer support, and brand protection.

EVIDENCE TO RETAIN

Evidence package, abuse reports, provider responses, browser-report submissions, customer notices, legal filings, and post-incident review.

REVIEW CADENCE

Quarterly runbook review, with event-based updates after takedown activity.

KEY METRIC

Time from detection to victim-traffic interruption and time to content removal or suspension.

A 30/60/90 Starting Sequence

Executive view

This sequence is designed for organizations that want practical risk reduction without waiting for a large transformation program.

The first 30 days focus on the highest-risk control gaps. Days 30 to 60 build monitoring and reduction workflows. Days 60 to 90 turn the work into an owned, repeatable operating model.

The 90-day outcome is to move public exposure, identity risk, brand impersonation, and recovery-path weakness out of the category of "assumed handled" and into the category of owned controls.

DAYS 0–30 Close the highest-risk control gaps

Outcome: the organization reduces the easiest paths for spoofing, account recovery bypass, internet-facing exploitation, and domain-control failure.

Move DMARC toward enforcement. Identify legitimate senders, fix SPF and DKIM alignment, and plan the move from monitoring to quarantine and reject.

Inventory internet-facing assets, DNS records, certificates, cloud accounts, SaaS tenants, and exposed admin portals.

Patch or mitigate anything on the CISA Known Exploited Vulnerabilities list that applies to your environment, starting with internet-facing systems. Use EPSS to prioritize exposed vulnerabilities that sit outside KEV.

Confirm MFA coverage. Deploy phishing-resistant MFA for administrators, identity owners, domain owners, executives, finance, HR, and developers with production access.

Remove SMS as a backup or recovery method for privileged and high-risk accounts.

Adopt or improve an enterprise password manager. Prefer a solution with strong enterprise controls, passkey support, hardware-key support, auditability, and a personal or family benefit for employees.

Enable registrar MFA, registrar lock, and alerts for domain, DNS, contact, and transfer changes.

Begin an OSINT footprint review for the organization and its high-risk people.

DAYS 30–60 Build monitoring and exposure-reduction workflows

Outcome: the organization starts seeing new public exposure, credential exposure, brand impersonation, browser risk, and recovery-path weakness before they become crises.

Stand up CT-log, newly registered domain, and lookalike-domain monitoring with Unicode and ASCII confusable matching.

Begin credential-leak, public-secret, paste-site, code-hosting, and data-broker monitoring.

Register the obvious defensive domain variants.

Audit phone-number exposure. Move public business lines to hardened managed VoIP where appropriate, verify the controlling account and recovery chain, remove direct mobile numbers from public materials, and apply carrier protections for high-risk mobile numbers.

Offer sponsored personal or family password manager accounts to employees where the chosen vendor supports it. Communicate clearly that personal vaults remain personal, while corporate secrets belong in managed business vaults.

Harden employee browser posture. Enforce updates, restrict extensions, separate work and personal profiles, and deploy a privacy-protective browser configuration.

Verify immutable backups and run at least one real restore drill.

Add CAA records and registry lock for the most important domains.

Review document metadata, public cloud storage, SaaS sharing, exposed repositories, and AI-tool data exposure.

DAYS 60–90 Make the work owned and repeatable

Outcome: the organization can show who owns each control, how it is reviewed, and what evidence proves it is still working.

Centralize high-value logs and wire up the short alert list for identity, email, DNS, registrar, SaaS, browser, cloud, and data movement events.

Run tabletop exercises covering ransomware, BEC, SIM swap, domain impersonation, public secret exposure, browser extension compromise, and sensitive-data exposure through AI tools.

Create or refresh takedown runbooks for domains, fake profiles, fake ads, fake support channels, and phishing pages.

Review third-party public exposure, including case studies, testimonials, vendor pages, partner directories, and event materials.

Create ownership and review cadence for each control. Assign named owners for domain security, identity, password management, browser security, OSINT exposure, backups, vulnerability management, logging, vendor exposure, and executive protection.

Quick Reference

IDENTITY AND RECOVERY

Phishable MFA

Use FIDO2 security keys, managed passkeys, or platform passkeys for privileged and high-risk accounts.

SIM swap

Remove SMS recovery, use carrier locks and PINs, avoid public mobile numbers, and move primary business lines only to VoIP tenants with phishing-resistant administrator access, hardened recovery, change alerts, and port controls.

Password reuse

Deploy an enterprise password manager with business vaults, personal vault separation, and sponsored family or personal use where available.

Legacy authentication

Disable protocols and flows that bypass modern MFA.

Reused and leaked credentials

Monitor breach data, block compromised passwords, and force resets when credible hits appear.

DOMAINS AND BRAND TRUST

Spoofed email as your domain

Move DMARC to `p=reject` after authenticating legitimate senders.

Lookalike domains

Monitor CT logs, newly registered domains, passive DNS, and confusable variants.

Domain hijack

Enforce registrar MFA, registrar lock, registry lock, CAA, DNSSEC where operationally safe, and change alerts.

Dangling subdomains

Tie DNS cleanup to cloud teardown and continuously verify third-party CNAME targets.

PUBLIC EXPOSURE

Exposed services

Run threat-actor-style self-recon with Shodan, Censys, CT logs, search engines, passive DNS, and cloud inventory.

Public data leakage

Audit cloud storage, SaaS sharing, document metadata, public links, AI-tool use, and vendor-published information.

Leaked secrets

Scan public repositories, add pre-commit and CI scanning, and rotate exposed credentials.

Executive targeting

Reduce public personal details, harden personal and corporate accounts, protect phone numbers, and monitor impersonation.

Vendor exposure

Govern vendor publication rights, case studies, screenshots, logos, architecture references, and partner-page details.

OPERATIONAL RESILIENCE

Known-exploited vulnerabilities

Prioritize CISA KEV. Use EPSS for the non-KEV long tail, adjusted for exposure and asset criticality.

Weak browser posture

Manage browsers, restrict extensions, block avoidable tracking and malvertising, and separate work and personal browsing.

Ransomware impact

Maintain immutable backups and test restores.

Slow incident response

Run tabletop exercises and maintain practical runbooks.

Standards and References

The controls in this guide rest on public standards and data sources. Cite them when a roadmap, vendor conversation, or board paper needs authority behind a recommendation.

THE FRAMEWORK

ODSF

The OSINT Defense & Security Framework, the controls-based model this guide applies. Five focus areas, FA1 through FA5, with subcategories and controls published at psysecure.com/odsf.

IDENTITY AND AUTHENTICATION

NIST SP 800-63B

The digital identity guidelines. The current revision classifies phone-based one-time codes as restricted authenticators.

FIDO2 and WebAuthn

The FIDO Alliance and W3C specifications behind security keys and passkeys.

EMAIL AUTHENTICATION

DMARC

RFC 9989, with aggregate reporting in RFC 9990 and failure reporting in RFC 9991. Together they replace RFC 7489.

SPF

RFC 7208, including the 10-DNS-lookup limit that constrains record design.

DKIM

RFC 6376, the cryptographic signature that DMARC alignment depends on.

MTA-STS and TLS reporting

RFC 8461 and RFC 8460, transport security and reporting for mail in transit.

DOMAINS AND CERTIFICATES

CAA

RFC 8659, the DNS record that restricts which certificate authorities may issue for a domain.

Certificate Transparency

RFC 9162, the public certificate-log ecosystem this guide uses for monitoring.

Confusables

Unicode Technical Standard #39, Unicode Security Mechanisms, including the skeleton algorithm for confusable matching.

Domain disputes

ICANN UDRP and URS, the trademark routes for domain recovery and suspension.

VULNERABILITY AND DISCLOSURE

CISA KEV

The Known Exploited Vulnerabilities catalog, the first input for patch priority on internet-facing systems.

EPSS

The FIRST Exploit Prediction Scoring System, with daily exploitation-likelihood scores for published CVEs.

security.txt

RFC 9116, the published security contact that shortens external reporting paths.

The Business Promise

Reduce the public information threat actors use before it becomes a crisis.

Most organizations already have many of the right controls. The problem is that those controls are often fragmented across teams, allowed to drift, or weakened by public information no one owns.

Threat actors exploit those gaps. They use exposed phone numbers, recovery paths, leaked credentials, lookalike domains, vendor oversharing, job posts, public documents, executive profiles, and personal details to make their attacks more believable and harder to stop.

PsySecure helps organizations turn that exposure into something governable.

Through Executive Exposure Advisory, ODSF Implementation, and OSINT Defence Training, we help executive teams and security leaders identify what threat actors can learn, reduce what they can use, and build evidence that the organization is actively managing public exposure risk.

The doctrine is operational:

> Exposure is not managed by intent. It is managed by ownership, reduction, monitoring, and response.

The outcome is practical:

> Fewer easy attack paths. Better executive protection. Stronger control confidence. Clearer board reporting.

To explore a private Executive Exposure Advisory review, ODSF readiness assessment, or OSINT Defence briefing, contact PsySecure at psysecure.com.

PsySecure

PRIVATE BRIEFING

REDUCE WHAT THREAT ACTORS CAN LEARN, IMITATE, AND ABUSE.

Three ideas this guide keeps returning to.

01 **Reconnaissance is the first move. Public exposure is the target.**

02 **A control nobody owns after deployment has already begun to drift.**

03 **A recovery path is part of the authentication system.**

Request a private briefing at **psysecure.com**.

Version 2026.06