

Padgett-Beale Inc Case Study

Posted on May 4, 2020

The Padgett-Beale case is best understood as an insider-risk and information-governance problem rather than simply an example of one dishonest employee. The scenario describes a departing employee with access to confidential future-development information who appears to have downloaded a large volume of material and transferred it to a personal cloud account. Because the employee had legitimate access to at least some of the files through committee responsibilities, the event illustrates a central insider-risk challenge: authorized access can still be misused, and ordinary perimeter defenses may not detect a valid user moving data in an unauthorized way.

The organization therefore has two tasks. First, it must respond to the suspected incident in a manner that preserves evidence, limits additional loss, respects legal and employee-rights requirements, and determines what information was actually exposed. Second, it must correct the organizational weaknesses that made excessive access, personal-cloud transfer, and delayed detection possible. Current NIST guidance treats cybersecurity as an enterprise-governance issue rather than an IT-only problem, while CISA's insider-risk materials emphasize preparation across people, information, and infrastructure (NIST, 2024; CISA, 2026).

Case Assessment: What the Evidence Suggests and What It Does Not Yet Prove

The combination of large downloads, departure from the organization, and transfer to a personal cloud service is a high-risk pattern that justifies investigation. It does not, by itself, prove theft, intent to benefit a competitor, or unlawful disclosure. An employee may have copied information for several possible reasons, including improper personal retention, convenience, backup, misunderstanding of policy, or deliberate exfiltration. The organization should therefore distinguish between indicators and conclusions.

The information itself must also be classified. Padgett-Beale appears to hold future property plans, acquisition information, financial projections, architectural concepts, vendor negotiations, market studies, and development strategy. Some of these materials may qualify as trade secrets if they derive economic value from not being generally known and if the company takes reasonable measures to protect them. Other material may instead be confidential business information protected by contract or internal policy. Trademark registration would not protect this type of information, and copyright or patent law would apply only to particular assets. The legal tool must match the asset.

The employee's authorization history is central. Membership on a planning committee may justify access to some strategic material, but it does not automatically justify unlimited download or

indefinite retention. If the employee retained permissions from earlier roles, could access unrelated projects, or could export large quantities without review, the incident reveals an access-governance failure regardless of the employee's intent. Least privilege means access should correspond to current business need, not simply to what the system technically allows.

Personal cloud storage creates a separate control failure. Once corporate files move into a personal account, the company may lose control of retention, access, deletion, sharing, encryption keys, and legal discovery. Even if the employee never sends the files to another party, the transfer itself can violate policy or contractual obligations. A mature environment should make approved collaboration easier than unauthorized workarounds while detecting or blocking high-risk transfers.

The First Response Should Preserve Evidence Before Making Accusations

Padgett-Beale's immediate response should be coordinated across cybersecurity, legal counsel, HR, privacy, records management, and the relevant business leadership. NIST SP 800-61 Revision 3, finalized in 2025, emphasizes integrating incident response across the full cybersecurity risk-management program rather than treating response as a narrow technical stage after detection (Nelson et al., 2025). For this case, evidence preservation should begin before investigators alter the employee's laptop, cloud configuration, or account history.

Relevant evidence may include endpoint logs, authentication records, file-access events, download history, email, approved cloud activity, browser history, data-loss-prevention alerts, badge records, device telemetry, and system timestamps. Investigators should establish a documented chain of custody for forensic copies where litigation or disciplinary action is possible. The original device should not be casually searched by a manager who could unintentionally modify timestamps, delete evidence, or create questions about the integrity of the investigation.

Access should be contained in proportion to risk. If the employee has already departed, corporate accounts, remote access, badges, tokens, privileged credentials, and shared secrets should be disabled or rotated as appropriate. If separation is still in progress, the timing of containment should be coordinated with HR and counsel. A high-risk departure may justify immediate restriction, but the organization should follow established policy rather than improvise.

The company should then determine the scope of exposure. Which files were downloaded? Were they all connected with legitimate committee work? Were archives created? Did uploads occur to one personal service or several? Were external sharing links created? Were files opened from another device after upload? Did the employee send messages suggesting transfer to a competitor? The answers affect both technical response and legal strategy.

The competitor's involvement should not be assumed from circumstantial evidence. If evidence

supports concern that another company received or solicited confidential information, counsel can consider preservation notices, cease-and-desist correspondence, civil remedies, or referral to law enforcement where appropriate. Premature public accusations could expose Padgett-Beale to legal and reputational risk. The investigation should therefore separate verified facts from hypotheses at every stage.

The Control Failure Is Broader Than the Employee

The most important lesson is that a firewall and password policy cannot prevent an authorized user from misusing legitimate access. Padgett-Beale needs controls centered on identity, data, and business context. NIST's zero-trust architecture rejects implicit trust based solely on being inside the corporate network. Authentication and authorization should be tied to the user, device, resource, and current context, with no assumption that network location itself makes an action trustworthy (Rose et al., 2020).

Access governance. Sensitive repositories should have named owners and defined access groups. Permissions should be reviewed when employees join, move between roles, enter temporary committees, or leave the organization. Temporary project access should expire automatically where possible. Managers should certify business need because IT administrators may know who can access a folder without knowing who should access it.

Data classification. Information cannot be protected effectively if the organization has not identified what matters most. Padgett-Beale should classify future-development plans, acquisition targets, financial models, contracts, customer information, architectural documents, and other sensitive material according to business impact and legal requirements. Classification should influence storage, sharing, retention, external access, and logging rather than exist only as a label.

Data-loss prevention. DLP controls can identify unusually large downloads, uploads to personal cloud services, sensitive file labels, external email attachments, removable-media copying, or anomalous sharing. Controls should be tested carefully because overly aggressive blocking can interfere with legitimate collaboration. High-risk alerts should include context such as user role, file sensitivity, transfer destination, recent job change, and whether the activity is typical for that user.

Managed collaboration. Employees need approved tools for sharing large files with architects, vendors, regional managers, and advisers. Blocking personal cloud services without providing usable alternatives encourages workarounds. Secure workspaces can include controlled membership, logging, expiring links, download restrictions, watermarking where justified, and external-sharing approval for especially sensitive projects.

Endpoint and removable-media controls. Corporate devices should use encryption, endpoint detection, patch management, managed configuration, and restrictions on unauthorized storage devices where risk warrants them. USB activity can be logged or limited to approved encrypted

media. These controls are more reliable than relying on guards or bag searches to identify every possible storage device.

Logging and detection. Authentication, file access, downloads, sharing changes, cloud uploads, endpoint copying, privileged actions, and physical entry should be logged with synchronized time. Logs need sufficient retention to investigate events that may not be discovered until after an employee leaves. Collecting logs without alerting, ownership, or review creates the appearance of control without the operational benefit.

Insider-Risk Governance Must Protect Both the Company and Employees

An insider-risk program can itself become harmful if it treats ordinary behavior as evidence of disloyalty. Working late, expressing frustration, seeking another job, or downloading files for an approved deadline does not prove theft. CISA's current insider-threat resources emphasize structured mitigation and reporting rather than arbitrary suspicion. Alerts should trigger human review using multiple sources, and security teams should distinguish between negligence, policy violations, compromised credentials, and intentional malicious behavior.

Privacy boundaries should be defined before an incident. Employees should know what corporate systems are monitored, how long records are retained, and which teams can access monitoring data. Investigators should not demand access to unrelated personal accounts or devices without appropriate legal authority. The goal is accountability for corporate information, not unrestricted surveillance of employees' private lives.

Managers have a specific governance role. They are often the first people to know that an employee changed assignments, joined a sensitive project, no longer needs a repository, or is preparing to leave. They should review access and report concerns through established channels rather than conduct their own covert investigation. Cybersecurity, HR, privacy, legal, and records-management teams should define escalation procedures before a crisis.

Offboarding should be treated as a security process. Accounts, remote access, badges, devices, corporate cards, shared credentials, file ownership, external collaboration links, and retention obligations should be reviewed systematically. The departing employee should receive a clear reminder of continuing confidentiality obligations and a lawful method to return or delete corporate data that may exist in approved personal locations. Contractors and consultants should be included in the same lifecycle controls.

A Better Padgett-Beale Program Can Be Mapped to Current NIST Practice

NIST Cybersecurity Framework 2.0 added stronger emphasis on governance and treats cybersecurity risk alongside other enterprise risks such as finance, reputation, and operational continuity. Padgett-Beale can use the six CSF functions—Govern, Identify, Protect, Detect, Respond, and Recover—to structure the insider-risk program rather than purchase isolated tools without an operating model (NIST, 2024).

CSF function	Application to the Padgett-Beale case
Govern	Define insider-risk authority, privacy rules, data ownership, escalation, legal roles, and executive accountability.
Identify	Inventory sensitive development information, map repositories, classify assets, and identify excessive access.
Protect	Apply least privilege, multifactor authentication, managed collaboration, endpoint controls, and secure offboarding.
Detect	Monitor bulk downloads, unusual cloud uploads, sharing changes, removable media, and anomalous access patterns.
Respond	Preserve evidence, contain access, investigate scope, coordinate HR/legal action, and communicate according to policy.
Recover	Restore secure operations, rotate compromised secrets, revise exposed plans where necessary, and correct control weaknesses.

This structure prevents the organization from treating the case only as an employee-discipline issue. If the investigation confirms that a worker copied sensitive plans, accountability is necessary, but punishing the individual without fixing permissions, cloud controls, logging, and offboarding leaves the same pathway available to the next employee or compromised account.

NIST's 2025 incident-response guidance reinforces this broader view by integrating preparation, detection, response, and recovery across the CSF. Lessons learned should therefore feed back into governance. Padgett-Beale should ask why the employee could accumulate or retain the access, why the download volume was not detected sooner, whether approved tools met legitimate collaboration

needs, and whether managers had a reliable process for removing temporary permissions.

The Padgett-Beale case ultimately demonstrates that intellectual-property protection depends on both legal rights and operational behavior. A trade secret is easier to defend when the company can show that it used reasonable protective measures: access restrictions, confidentiality agreements, secure storage, classification, training, monitoring, and consistent enforcement. Technology does not replace these measures, and contracts do not replace technical controls.

The strongest response is therefore evidence-driven and systemic. Padgett-Beale should preserve and investigate the suspected incident, contain remaining access, determine what information left corporate control, and use counsel to decide what legal action is justified. It should then redesign access and data governance around least privilege, secure collaboration, DLP, endpoint security, logging, reliable offboarding, and privacy-aware insider-risk review. A mature program does not assume every employee is untrustworthy. It makes legitimate work easy, sensitive access accountable, and unusual movement of critical information visible before a departure turns into a crisis.

References

- Cybersecurity and Infrastructure Security Agency. (2026). *Insider Threat Mitigation Resources and Tools*.
- National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*.
- Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile* (NIST SP 800-61 Rev. 3).
- Rigopoulos, K., Quinn, S., Pascoe, C., Marron, J., Mahn, A., & Topper, D. (2024). *NIST Cybersecurity Framework 2.0: Resource & Overview Guide* (NIST SP 1299).
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST SP 800-207).