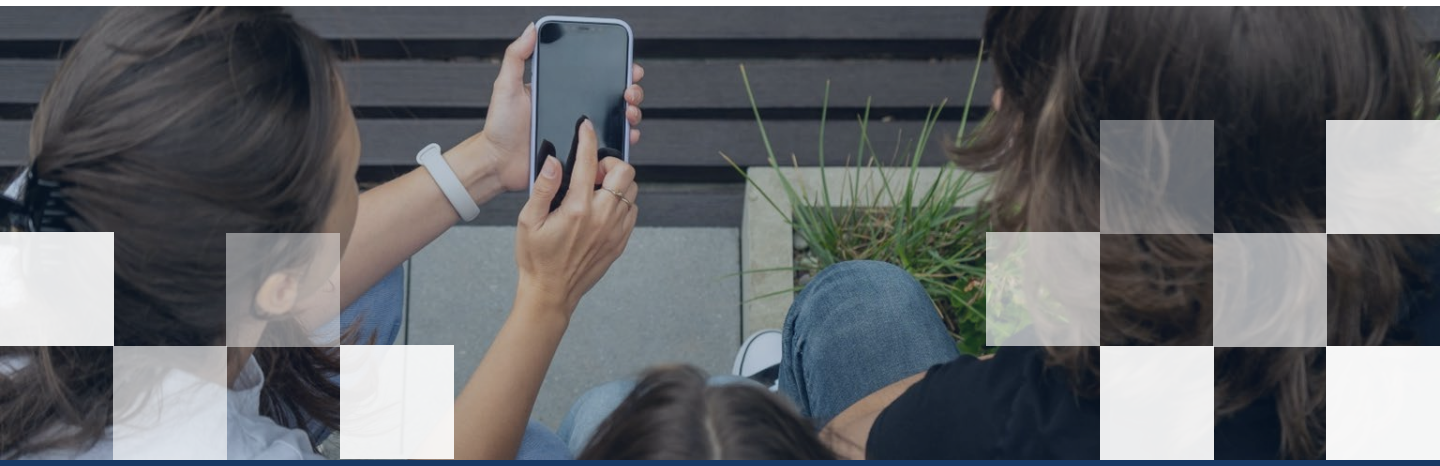
The Digital Dimension of Individuals and Families: A Governance Framework

Authored by: Caroline Sacks, Ariel Fortunato, Lucas Fisher



Insights from Brown Advisory

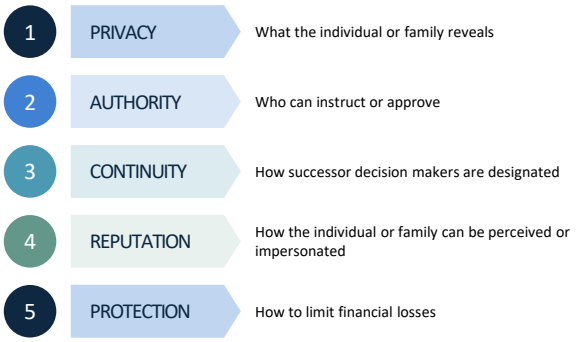
Fast Reading:

- AI-enabled impersonation and social engineering now target identity, access and trust as much as technology, making digital stewardship a core governance issue, not just an IT task.
- A digital footprint determines who can see information, approve activity, move money and communicate in the individual and family's name, so informal digital habits can create vulnerabilities across privacy, authority, continuity, reputation and protection.
- Embedding digital stewardship into a governance framework and making verification routine can clarify decision rights, strengthen resilience and better protect multigenerational continuity.
- To help individuals and families turn these ideas into action, we created a Digital Safety & Governance Meeting Checklist for quarterly reviews, major life changes and new accounts, devices, advisers or employees. Addressing the Priority Actions laid out in the checklist can materially reduce risk.

Cybersecurity used to sit at the edge of individual and family planning. Many treated it as a technical issue to delegate to an IT provider, a household employee or the most digitally fluent person in the room. That posture no longer fits the threat environment. The Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) reported more than $20.8 billion in losses from cyber-enabled crime in 2025.[1] Verizon's 2025 Data Breach Investigations Report (DBIR) analyzed 12,195 confirmed breaches across 139 countries and found that human involvement remained a factor in about 60% of breaches, third-party involvement doubled from the prior year and ransomware appeared in 44% of breaches.[2] Microsoft has also warned that generative artificial intelligence (AI) is increasing the scale and persuasiveness of social engineering campaigns.[3] In this environment, cyber resilience requires more than informal delegation; it requires practical governance. We help build that governance, and our checklist can help operationalize the discussion by translating broad priorities into concrete action.

The modern attack often targets trust before it targets technology. Attackers spoof domains, clone voices, hijack email threads and manufacture urgency. In 2025, the FBI warned that malicious actors were using AI-generated voice messages and texts to impersonate senior U.S. officials, establish rapport and steer targets to secondary platforms or malicious links.[4] In a separate alert, the FBI said that account-takeover fraud tied to impersonation of financial institution support generated more than 5,100 complaints and more than $262 million in reported losses since January 2025.[5]

For ultra-high-net-worth (UHNW) individuals and families, this shift changes the frame: the evolution of cyber threats from technical vulnerabilities to attacks on identity, access and trust elevates cybersecurity into a central concern of governance. A digital footprint is the living system of identities, devices, records, permissions, communication channels and public visibility that shapes who can see information, approve activity, move money, change instructions and speak credibly in the name of the individual and family. In other words, digital life now touches the same issues that governance has always tried to address:



Why a Digital Culture Belongs in Governance

**The better question isn't, "Are our tools secure?"
It's, "How is this family organized to manage digital trust?"**

Governance is about stewardship. It assigns roles, clarifies decision rights, sets oversight and prepares a family to respond when something goes wrong. That same logic now applies to digital life.

That distinction matters because many individuals and families formalize the governance of capital long before they formalize the governance of digital exposure. They may have clear structures for trusts, entities, philanthropy and succession, yet still rely on informal password sharing, ambiguous approval authority or unverified instructions delivered through text messages or messaging apps. In a world shaped by spoofing, impersonation and AI-enhanced social engineering, familiarity is no longer a control. Process and governance are.

The governance challenge is especially acute for those whose lives operate more like small enterprises than single households. Many UHNW individuals and families coordinate multiple residences, entities, outside advisers, employees and several generations with different responsibilities. Our own work with these clients notes that many find it useful to think of these arrangements as a type of business whose success depends on common purpose and culture. Once an individual or family starts to look like a system, digital risk stops being a side issue. One weak point can affect privacy, trust, operations and control far beyond the individual level.

A 2026 Framework for Digital Governance

We see that individuals and families make better decisions when they translate complexity into a practical framework. For 2026, those broader governance themes become most useful when translated into five practical meeting questions:

Dimension	Core Question	What Good Governance Looks Like
Awareness	**What are we exposing?**	Map the digital footprint: accounts, communications, devices, shared drives, password managers, assistants, vendors, household systems and public information that could support impersonation or credential reset.
Access	**Who can get in?**	Review permissions across personal, household, philanthropic, business and entity systems. Remove stale access, reduce administrator rights and separate credentials by role.
Authority	**Who can act?**	Distinguish support from authorization. Someone may need to schedule travel, assemble records or pay routine bills without having authority to reset credentials, approve wires or change standing instructions.
Authenticity	**How do we verify?**	Establish trusted channels for sensitive requests and define when a callback, second channel or dual approval is required. In an era of cloned voices and convincing spoofing, verification is a control, not a courtesy.
Action	**Who responds?**	Create a short incident playbook. If a device is lost, an account is compromised or a suspicious request arrives, individuals and families should know who freezes activity, who contacts institutions, who documents the event and who coordinates with outside specialists.

From Concern to Culture

A framework only works if people use it. We have long emphasized education, next-generation engagement and the role of family meetings in long-term stewardship. The same principle now applies to digital judgment. We believe establishing shared norms, such as pausing when a request feels unusually urgent, verifying changes in instructions and recognizing that convenience can introduce risk, can help individuals, families, assistants and household employees navigate an increasingly complex digital environment. Good governance creates a culture where pausing to verify is expected. This is one way the next generation, who is often more comfortable with technology, can contribute meaningfully to family governance, by helping the family navigate new digital realities. A family is stronger when they are working across all of the different systems, bringing them together for a shared purpose. The downloadable checklist is meant for exactly this kind of conversation, bringing senior and rising-generation voices into one practical review without requiring deep technical fluency.

This does not mean every individual or family needs to become its own cybersecurity shop. It means they should place digital stewardship inside the same planning architecture that already governs liquidity, estate plans, philanthropy, succession and communication. We believe Brown Advisory's broader planning model is well suited to helping clients frame the right questions, clarify roles and escalation paths, and connect digital stewardship to the objectives of asset protection, continuity and multi-generational preparedness.

Closing Thought: The New Perimeter

The core mission of governance has not changed, though it needs to expand in scope to incorporate modern operating philosophies. It still aims to preserve wealth, prepare rising generations and protect continuity across time. But in 2026, the perimeter around those goals is digital as well as legal and financial. For successful individuals and families, a digital footprint is no longer background noise to modern life. It is part of the governance architecture that protects or exposes.

Our strategic advisors are thinking partners who help clients optimize tax, estate, generational, philanthropic and business planning, including asset protection strategies. That broader advisory lens matters here. Cyber risk does not sit outside an individual or family system. It moves through the same relationships, delegated roles and decision structures that shape the rest of governance.

A practical next step is to use the accompanying checklist to identify priorities, clarify roles and make digital stewardship a more regular part of governance. For many, the value is not in trying to do everything at once, but in beginning with the right conversations and a manageable set of actions. Our Strategic Advisory Group is available as a resource to help clients think through those priorities and use the checklist as a starting point to operationalize this practice.

Sources

1. Source: Internet Crime Complaint Center, "2025 IC3 Annual Report," as of 04/10/2026; https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf
2. Source: Verizon, "2025 Data Breach Investigations Report" and "2025 DBIR Executive Summary," as of 04/10/2026; https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf and https://www.verizon.com/business/resources/reports/2025-dbir-executive-summary.pdf
3. Source: Microsoft, "Microsoft Digital Defense Report 2025" and "CISO Executive Summary," as of 04/10/2026; https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/ and https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/security/CISO-Executive-Summary-MDDR-2025.pdf
4. Source: Internet Crime Complaint Center, "Senior US Officials Impersonated in Malicious Messaging Campaign," 05/15/2025; https://www.ic3.gov/PSA/2025/PSA250515
5. Source: Federal Bureau of Investigation, "Account Takeover Fraud via Impersonation of Financial Institution Support," 11/25/2025; https://www.fbi.gov/investigate/cyber/alerts/2025/account-takeover-fraud-via-impersonation-of-financial-institution-support