C-Suite Guidelines For Cybersecurity, Fraud Risk & Insurance

HOW TO EVALUATE THESE RISKS FOR
YOUR BUSINESS & YOUR PERSONAL LIFE

ABOUT THIS GUIDE

Today, cyber and payment fraud losses are board-level risks. Cyber insurance can be complex, but proper coverage can be essential to keeping your business operational and solvent when incidents occur. This guidebook is intended as a tool for executives, in businesses of all sizes, to help evaluate cyber and other fraud risks for their businesses. It has three parts.

- **Part I** presents diagnostic questions for executives to ask their teams and providers. It is designed to help executives test whether their organization's defenses, response readiness, and insurance posture are appropriate.
- **Part 2** provides a controls assessment that reveals strengths and areas of improvement for your business. It will help you prioritize controls based on the size and complexity of your business, and it will help you align your investments with cyber insurance carriers and regulators. The controls assessment is informed by current cyberthreat intelligence. This control assessment also provides a standardized material scale that will inform you where your cybersecurity and fraud risk programs are strong and where improvement may be needed.
- **Part 3** offers tailored recommendations for high-profile or high-net worth individuals who also need to consider protecting their personal lives from cyber and fraud-related threats.

PART I: QUESTIONS EVERY C-SUITE SHOULD ASK IT, SECURITY & KEY PROVIDERS

Purpose: To help you diagnose how prepared your business is to deal with cybersecurity and fraud issues, you should ask these questions of your information technology and cybersecurity vendors and your insurance providers.

1. **When was our last independent cybersecurity risk assessment, and what was the status of every high-priority finding?** If a cybersecurity assessment was completed longer than 12 months ago, or the assessment was not aligned with a broadly accepted standard/framework (e.g., NIST CSF, CIS, ISO 27001 or other), and an owner for each open item was not identified, this is a red flag.

2. **Is multi-factor authentication (MFA) enforced on every account?** Accounts include email, VPN, remote access, cloud admin consoles, and privileged users. Are there any exceptions and why? Ask specifically about non-human/service accounts, legacy protocols, and contractors. If you employ agentic AI, are agent identities identified and monitored? Incomplete coverage is a red flag.

3. **Do we have immutable, offline backups, or immutable backup technology with built-in ransomware protection, and when did we last successfully restore production systems from them?** Untested backups are not reliable. Ask for the recovery time objective (RTO) and determine if it aligns with your expectations to restore business operations. If backup testing is not performed regularly, or testing shows that restore operations extend longer than your expectations, this is a red flag.

4. **What is our incident response plan, who is on the call tree, and when did we last run a tabletop exercise that included stakeholders other than technical responders?** If a legitimate tabletop exercise has not been conducted in the last 12 months for a scenario that is relevant to your business, or you do not have a pre-negotiated retainer with an incident response (IR) firm and outside breach counsel, this is a red flag.

5. **Do we have 24/7 monitoring and response (e.g., by an internal team or a managed detection and response (MDR) third party), and what is our mean time to detect and contain an intrusion?** Ransomware now executes in hours, and identity-based attacks can progress from initial access to lateral movement in under 30 minutes. Detection windows measured in days are unacceptable. Organizations should expect to detect credible threats within minutes to an hour and contain them within the same operational window. If detection or containment takes multiple hours, attackers may already have achieved their objectives. Related to monitoring is visibility - your teams cannot protect what they cannot see. Ask if there are visibility gaps in logging that impact the ability to monitor.

6. **How do we manage third-party and vendor risk, including Software-as-a-Service (SaaS) providers and managed service providers with privileged access?** Most major breaches now originate in the supply chain. Ask about the onboarding process, key contract provisions, ongoing monitoring and termination processes. If third-party risk management is just a box-checking exercise, this is a red flag. The best approach is to stratify your supply chain by risk tiers and focus your efforts on where the risk is greatest. The supply chain is in constant motion and requires continuous oversight.

7. **What controls protect our wire transfers, ACH, and vendor master file changes from business email compromise (BEC) and payment fraud?** Look for dual approval, out-of-band callback

verification on any banking change, positive pay, and ACH debit blocks/filters. Cybercriminals are after your financial assets, and fraud controls have a high ROI. Ask how your IT/cyber teams protect against email threats that lead to BEC. Ask where the gaps in email security are as email remains the most common entry point for serious threats.

8. **Do our cyber and crime insurance policies cover our top exposures, and do we meet every control requirement listed in the policy applications?** Misrepresentations void coverage. Review sub-limits for ransomware, social engineering / electronic funds transfer, and business interruption with your insurance agent annually.

9. **What is our patch cadence for internet-facing systems, and how do we know it's being followed?** Ask for SLAs, the last vulnerability scan summary, and exception count. Patch cadence is increasingly important in the age of artificial intelligence. By the end of 2026, some experts predict that the time from vulnerability discovery to exploitation will be compressed to less than eight hours due to frontier AI capabilities.

10. **How often do employees, especially finance and executive assistants, receive phishing simulations and fraud-scenario training?** What are the failure rates trending toward? Trend matters more than any single number. Security awareness training is ineffective if it is not measured or if progressive corrective training is not implemented for users that repeatedly fail. Mature organizations target click-through rates below 3 to 5%, where lower is better.

11. **Has our security program been assessed against the risks posed by frontier AI—specifically autonomous vulnerability discovery, exploit chaining, and the collapse of the patch window?** Frontier AI models can now autonomously discover zero-day vulnerabilities across every major operating system and web browser, chain multiple lower-severity weaknesses into full compromise paths and generate working exploits. These are capabilities that were exclusive to elite nation-state actors just months ago. The average time from vulnerability disclosure to a working exploit has collapsed from 56 days in 2024 to approximately 10 hours in 2026, and in some cases, exploitation occurs before a patch is even available. Open-source software is particularly exposed because frontier AI is dramatically more effective when it can reason against source code. Since nearly all commercial software incorporates open-source components, this risk extends to your entire software stack. Ask your IT and security teams: Can we identify and patch critical vulnerabilities in hours, not weeks? Do we know what open-source components are embedded in our systems? Are we relying on traditional patch cycles that were designed for a threat environment that no longer exists? If the answer to any of these is uncertain, this is a red flag.

12. **Do we know where our sensitive data resides, who has access to it, and how it is protected?** Organizations cannot secure what they cannot see. Sensitive data, including customer information, financial records, and internal business data, often resides across endpoints, cloud services, third-party platforms, and employee workflows. Ask your IT and security teams how data is classified, where it is stored, and how access is controlled and monitored. If you cannot clearly identify where sensitive data exists and how it is protected from unauthorized access or exfiltration, this is a red flag.

PART 2: CONTROLS ASSESSMENT FOR EXECUTIVES & TECHNICAL TEAMS

Purpose: To provide you with a clear understanding of key controls needed to comply with most insurance requirements and to help protect your business against existing and emerging threats.

- Controls are organized into three functions: **Keep Them Out** (prevent attacks), **Catch Them Fast** (detect threats quickly), and **Limit the Damage** (contain impact and recover operations).
- Controls marked with  represent requirements commonly expected by cyber insurers and should be treated as baseline cyber-hygiene (e.g. focus on these first). The remaining controls define the capabilities needed to detect threats rapidly and limit business impact when controls fail.
- **Share this with your IT and security leaders. Ask them to check the box that indicates the maturity level for each control in your organization. Begin with the baseline cyber-hygiene controls. As your organization matures through the baseline controls you will have substantial protection against ransomware and other common threats. As your organization matures through the remaining controls, your business will be responsive and resilient in a complex, rapidly changing threat landscape—and covered by a well-planned insurance policy.**

SPEED IS NOW A CONTROL

Modern cyberattacks often move from initial access to lateral movement in under 30 minutes. Leading organizations detect threats in minutes and contain them within an hour. Response times measured in hours or days significantly increase financial and operational impact.

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
1	**Multi-Factor Authentication (MFA)**	**Keep them out** 	Phishing-resistant MFA (FIDO2/hardware tokens) on email, VPN, remote desktop, cloud admin, and all privileged accounts. No SMS for admins. This single control blocks most account-takeover attacks and is a hard requirement for cyber insurance. MFA prevents access when passwords/credentials are compromised.	☐ **Partial**	MFA exists on some systems; exceptions are undocumented; SMS-based for most users
				☐ **Risk-Informed**	MFA on email and VPN; exceptions are known but not formally managed; no phishing-resistant methods
				☐ **Repeatable**	MFA enforced on all accounts including privileged, cloud, and remote access; phishing-resistant (FIDO2) for admins; exceptions documented and approved

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
				☐ **Adaptive**	Phishing-resistant MFA universal; conditional access policies adapt based on risk signals; non-human/service account identities monitored; continuous coverage validation
2	**Privileged Access Management & least privilege**	**Keep them out**	Separate admin accounts from daily-use accounts, vault privileged credentials, enforce just-in-time elevation, and remove local admin rights from end users. Audit privileged activity. For enhanced security, consider FIDO2 password-less options with strong multi-factor authentication.	☐ **Partial**	Admins use daily accounts for privileged tasks; local admin rights common; no credential vaulting
				☐ **Risk-Informed**	Separate admin accounts exist but are not consistently enforced; some credential vaulting in place
				☐ **Repeatable**	All privileged credentials vaulted; just-in-time elevation enforced; local admin removed from endpoints; privileged activity audited regularly
				☐ **Adaptive**	Password-less/FIDO2 for privileged access; automated anomaly detection on privileged sessions; continuous least-privilege validation across cloud and on-prem
3	**Patch & vulnerability management**	**Keep them out**	Patch critical and internet-facing systems quickly. Due to the influence of AI, the time it takes to exploit a vulnerability will continue to decrease. Continuous external attack surface scanning is an important control but will not typically identify lower severity vulnerabilities that can be chained together to gain access. Vulnerability scanning should be continuous.	☐ **Partial**	Patching is reactive; no formal cadence; vulnerability scanning sporadic or absent
				☐ **Risk-Informed**	Monthly patch cycle exists; periodic vulnerability scans; no SLAs for remediation
				☐ **Repeatable**	Defined SLAs for critical/high/medium; continuous vulnerability scanning; internet-facing systems patched within days; exception tracking in place
				☐ **Adaptive**	Prioritization by exploitability and attack path (not just severity); SBOM maintained; critical patches deployed in

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
					hours; AI-augmented vulnerability analysis integrated
4	**Email security & anti–business email compromise**	**Keep them out** 	Advanced email filtering, DMARC/DKIM/SPF enforced, external-sender banners, auto-detection of inbox forwarding rules and look-alike domains. BEC is the #1 source of direct-dollar loss for mid-market firms. BEC often results from compromised, trusted accounts (e.g. vendors or customers), where detection is difficult. Ensure your IT/cyber teams know how to secure your email/communications environment. This is a gap that many small businesses overlook.	☐ **Partial**	Basic spam filter; no DMARC/DKIM/SPF; no external sender banners
				☐ **Risk-Informed**	DMARC in monitoring mode; external sender banners enabled; basic email filtering
				☐ **Repeatable**	DMARC enforced (reject); advanced email filtering with sandboxing; auto-detection of forwarding rules and look-alike domains; external banners active
				☐ **Adaptive**	AI-powered email threat detection; real-time link and attachment detonation; automated response to compromised mailboxes; continuous tuning based on threat intelligence
5	**Payment & treasury fraud controls**	**Keep them out** 	Dual approval on all wires and ACH originations, out-of-band callback verification on any vendor banking change (using a known number, never the one in the email), Positive Pay, ACH debit blocks/filters, and segregation of duties between vendor master file edits and payment release.	☐ **Partial**	Single-approval wire transfers; no callback verification; no positive pay
				☐ **Risk-Informed**	Dual approval on wires over a threshold; callbacks on some changes; positive pay on some accounts
				☐ **Repeatable**	Dual approval on all wires and ACH; out-of-band callback on all banking changes using known numbers; positive pay and ACH blocks/filters; segregation of duties between vendor master and payment release
				☐ **Adaptive**	Automated fraud detection integrated with payment systems; real-time anomaly alerting on transaction patterns; regular red-team testing of payment fraud controls

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
6	**Endpoint Detection & Response (EDR) with 24/7 monitoring**	**Catch them fast** 	Modern EDR/XDR backed by a Managed Detection & Response provider or internal SOC. Legacy antivirus alone will not stop ransomware. Required by nearly all carriers above $1 million in coverage. Mature programs achieve detection in minutes and containment within an hour for critical threats.	☐ **Partial**	Legacy antivirus only; no centralized monitoring; alerts reviewed during business hours
				☐ **Risk-Informed**	Modern EDR deployed on most endpoints; alerts reviewed but not 24/7; no MDR provider
				☐ **Repeatable**	EDR/XDR on all endpoints and servers; 24/7 MDR or internal SOC; detection in minutes; containment within an hour for critical threats
				☐ **Adaptive**	Automated containment actions; threat hunting integrated; detection tuned continuously based on adversary TTPs; full coverage including cloud workloads and mobile
7	**Centralized logging and monitoring (Security Information & Event Management (SIEM))**	**Catch them fast**	Centralized log aggregation across identity, endpoint, network, email, and cloud systems with a minimum 90-day hot retention and 1-year archival. Logs should be immutable or tamper-resistant. A SIEM or equivalent platform correlates events in real time and generates alerts for investigation. Without centralized logging, detection and response are blind, forensic investigations are incomplete, and cyber insurance claims may be unsubstantiated. Carriers now specifically ask about log coverage, retention, and monitoring as part of the underwriting process.	☐ **Partial**	Logs exist on individual systems but are not aggregated; no SIEM; no retention policy
				☐ **Risk-Informed**	Some log sources feed a SIEM; limited correlation rules; retention under 90 days
				☐ **Repeatable**	Centralized logging across identity, endpoint, network, email, and cloud; 90-day hot / 1-year archival; immutable or tamper-resistant logs; real-time correlation and alerting
				☐ **Adaptive**	AI-augmented correlation; automated triage and enrichment; continuous coverage validation; log integrity monitoring; integrated with IR playbooks for automated response
8	**AI-Powered Threat Defense**	**Catch them fast**	Maintain a current inventory for all applications and systems, with emphasis on open-source	☐ **Partial**	No awareness of AI as a threat vector; no AI inventory; no AI acceptable use policy

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
	& AI Governance		components. Prioritize vulnerabilities by exploitability, attack path, and asset criticality rather than severity score alone. Assume traditional patch cadences are insufficient for critical and internet-facing systems—target hours, not weeks. Deploy AI-augmented detection tools capable of identifying exploit chaining and anomalous lateral movement. If your organization uses AI internally, establish an AI acceptable use policy, inventory all AI tools in use (sanctioned and unsanctioned), and ensure AI-generated outputs are subject to human review before action. Incorporate AI-powered attack scenarios into tabletop exercises annually.	☐ **Risk-Informed**	Leadership aware of AI risks; informal inventory of AI tools; no AI-specific detection or governance
				☐ **Repeatable**	AI acceptable use policy in place; sanctioned and unsanctioned AI tools inventoried; AI-augmented detection deployed; AI attack scenarios included in tabletop exercises; human review required for AI-generated outputs
				☐ **Adaptive**	AI-powered detection of exploit chaining and anomalous lateral movement; SBOM integrated with AI vulnerability analysis; continuous assessment of AI threat landscape; AI governance integrated with enterprise risk management
9	**Security awareness & phishing simulation**	**Catch them fast**	Monthly simulated phishing with targeted training for repeat clickers. Consider specialized wire-fraud and deepfake-voice training for Finance, AP, Treasury, and Executive Assistants. Consider that even your help desk can get socially engineered—harden identity verification procedures for employees who call the help desk and then test the help desk. Measure the effectiveness of your training program.	☐ **Partial**	Annual compliance training only; no phishing simulations; no metrics
				☐ **Risk-Informed**	Quarterly phishing simulations; general awareness training; click rates tracked but not acted on
				☐ **Repeatable**	Monthly simulations with targeted training for repeat clickers; specialized training for Finance/AP/Executive Assistants; help desk social engineering tested; click-through rates below 3 to 5% and trending down
				☐ **Adaptive**	Adaptive simulations that adjust difficulty based on user performance; deepfake voice/video scenarios included; real-time teachable moments; training

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
					effectiveness measured and reported to leadership
10	**Immutable, tested backups (3-2-1-1-0)**	**Limit the damage** 	Best case: Three copies, two media, one offsite (or cloud), one immutable, zero errors on restore tests. Test restores quarterly. Variations may be acceptable if the immutable backups are distributed and contain built-in ransomware prevention technology. Your ability to restore operations quickly is the difference between paying a ransom and not.	☐ **Partial**	Backups exist but are not tested; no immutable copies; no defined RTO
				☐ **Risk-Informed**	Regular backups with some offsite storage; annual restore test; RTO defined but not validated
				☐ **Repeatable**	3-2-1-1-0 implemented; quarterly restore tests with zero errors; immutable or air-gapped copies; RTO validated and aligned with business expectations
				☐ **Adaptive**	Automated restore validation; ransomware-specific backup integrity monitoring; RTO continuously tested against evolving threat scenarios; backup coverage reviewed when systems change
11	**Network segmentation & Zero Trust principles**	**Limit the damage**	Separate corporate, guest, payment, and operational technology networks. Limit lateral movement. The castle-and-moat approach to security is no longer sufficient, meaning do not limit your concept of risk to only what is outside your network. Assume breach and verify every access request to company resources, internally and externally (zero-trust approach).	☐ **Partial**	Flat network; no segmentation between corporate, guest, or payment systems
				☐ **Risk-Informed**	Basic segmentation (e.g., guest Wi-Fi separated); firewall rules exist but are not regularly reviewed
				☐ **Repeatable**	Corporate, guest, payment, and OT networks segmented; lateral movement restricted; access requests verified regardless of network location (zero-trust approach)
				☐ **Adaptive**	Micro-segmentation; continuous access verification with adaptive policies; automated isolation of compromised segments; zero-trust architecture fully implemented across cloud and on-prem

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
12	**Third-party / vendor risk management + incident response readiness**	**Limit the damage**	Documented vendor risk program with security requirements in contracts and ongoing monitoring of third-party security posture. Stratify vendors by risk tier and focus assessment effort where access to sensitive data or critical systems is greatest. Ensure visibility into vendor access, data handling practices, business continuity, and dependency on critical third-party systems. Run a tabletop annually that incorporates scenarios involving third-party compromise.	☐ **Partial**	No formal vendor risk program; security not addressed in contracts
				☐ **Risk-Informed**	Vendor risk questionnaires sent at onboarding; security clauses in some contracts; no ongoing monitoring
				☐ **Repeatable**	Vendors stratified by risk tier; security requirements in all contracts; periodic reassessment of high-risk vendors; visibility into vendor access and data handling
				☐ **Adaptive**	Continuous vendor risk monitoring; automated alerts on vendor security incidents; third-party compromise scenarios included in tabletop exercises; vendor risk integrated with enterprise risk management
13	**Incident Response Readiness & Execution**	**Limit the damage**	Tested incident response plan with a defined call tree, decision authority, and pre-engaged third parties, including an incident response firm, breach counsel, and forensic resources. Conduct at least one tabletop exercise annually that includes executive leadership and scenarios involving ransomware, business email compromise, and third-party compromise. Response procedures should enable containment actions (e.g., disabling accounts, isolating systems) within minutes, not hours.	☐ **Partial**	No documented IR plan; response is improvised; no pre-engaged third parties
				☐ **Risk-Informed**	IR plan exists but has not been tested; call tree defined; no retainer with IR firm or breach counsel
				☐ **Repeatable**	Tested IR plan with defined call tree and decision authority; pre-engaged IR firm, breach counsel, and forensic resources; annual tabletop with executive leadership; containment actions executable within minutes
				☐ **Adaptive**	Automated containment playbooks; IR plan updated after every incident and exercise; lessons learned integrated into detection rules; cross-functional exercises include ransomware, BEC, and third-party compromise scenarios

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR ORGANIZATION'S MATURITY	
14	**Data Security & Resilience (Classification, Encryption, DLP)**	**Limit the damage**	Classify sensitive data and enforce encryption in transit and at rest across systems, endpoints, and cloud services. Implement data loss prevention (DLP) controls to detect and block unauthorized transmission of sensitive information across email, web, endpoints, and cloud applications. Restrict access to sensitive data based on least privilege and monitor for anomalous access or exfiltration activity. Organizations should understand where their sensitive data resides, who can access it, and how it leaves the environment. Failure to maintain visibility and control over sensitive data materially increases financial, regulatory, and reputational impact of a breach.	☐ **Partial**	No data classification scheme; encryption inconsistent; no DLP controls
				☐ **Risk-Informed**	Data classification policy exists but is not consistently applied; encryption on some systems; basic DLP on email
				☐ **Repeatable**	Sensitive data classified and labeled; encryption enforced in transit and at rest; DLP controls across email, web, endpoints, and cloud; access restricted by least privilege; anomalous access monitored
				☐ **Adaptive**	Automated data discovery and classification; real-time DLP with adaptive policies; continuous monitoring for exfiltration; data security posture integrated with SIEM and IR workflows

PART 3: WHAT SHOULD YOU BE DOING PERSONALLY? CONSIDERATIONS FOR HIGH-PROFILE OR HIGH NET-WORTH INDIVIDUALS

Purpose: To provide you with proven risk mitigation strategies for your personal data and assets. High-profile and high-net-worth individuals are disproportionately targeted by cybercriminals because their personal accounts, relationships, and public visibility offer direct access to financial assets and sensitive information. The same threat actors targeting your business are also targeting you personally.

As a potential target of fraud, you should focus attention on monitoring your identity, securing your login credentials, monitoring your financial transactions, patching your personal devices, securing your communications and obtaining the right insurance. The controls listed below will help you do that. The maturity scale will tell you where you are at today and improvements you should make based on your personal risk tolerance. Consider extending these controls to household members and trusted advisors, since attackers frequently target family members as a path to the primary individual.

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY	
1	**Personal identity monitoring**	**Catch them fast**	Enroll in a reputable identity monitoring service that covers credit bureau alerts, dark web surveillance, and public records changes. Place a credit freeze with all three major bureaus (Equifax, Experian, TransUnion) and lift it only when needed. Review your credit reports at least annually. For high-profile individuals, consider executive identity protection services that monitor for impersonation, doxxing, and exposure of personal information on data broker sites. Consider a service that removes your information automatically from data broker sites, subject to your consent. If you are not actively monitoring for misuse of your identity, you may not discover fraud until significant damage has occurred.	☐ **Partial**	No credit monitoring; credit not frozen; no awareness of dark web exposure
				☐ **Risk-Informed**	Credit monitoring through one bureau; credit freeze not in place; no dark web monitoring
				☐ **Repeatable**	Credit frozen at all three bureaus; identity monitoring service active with dark web and public records alerts; credit reports reviewed annually; data broker opt-outs completed
				☐ **Adaptive**	Executive identity protection service in place; continuous dark web and impersonation monitoring; automated alerts on public records changes; proactive data broker removal on a recurring basis
2	**Personal credential security & multi-**	**Keep them out**	Use a reputable, end-to-end encrypted password manager to generate and store unique,	☐ **Partial**	Passwords reused across accounts; no password

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY	
	factor authentication		complex passwords for every personal account. Enable multi-factor authentication (MFA) on all accounts that support it — especially email, banking, investment, and social media. Use phishing-resistant MFA for your most sensitive accounts. Never reuse passwords across personal and business accounts. If your personal email is compromised, attackers can use password reset flows to take over banking, brokerage, and other critical accounts.		manager; MFA not enabled on most accounts
				☐ **Risk-Informed**	Password manager in use for some accounts; MFA enabled on banking and email; some password reuse remains
				☐ **Repeatable**	Password manager used for all accounts; unique passwords everywhere; MFA enabled on all accounts that support it; phishing-resistant MFA on email, banking, and investment accounts
				☐ **Adaptive**	Phish-resistant MFA for primary email and financial accounts; passkey/FIDO2 adoption where supported; password manager audited for weak or reused credentials; family members included in credential hygiene practices
3	**Financial transaction monitoring & fraud alerts**	**Catch them fast**	Enable real-time transaction alerts on all bank accounts, credit cards, and investment accounts. Set dollar thresholds for alerts that match your risk tolerance. Review statements monthly and dispute unauthorized transactions promptly. For high-net-worth individuals, coordinate with your financial advisor and private banker to establish callback verification procedures for any large transfers or changes to account instructions. Wire fraud targeting personal accounts is increasing — particularly through compromised email and social engineering of financial advisors.	☐ **Partial**	No transaction alerts enabled; statements not regularly reviewed; no callback procedures with financial institutions
				☐ **Risk-Informed**	Transaction alerts on primary bank accounts; monthly statement review; no callback verification for large transfers
				☐ **Repeatable**	Real-time alerts on all financial accounts with defined thresholds; monthly statement review; callback verification established with financial advisor and private banker for transfers and account changes
				☐ **Adaptive**	Automated anomaly alerts across all accounts; coordinated fraud monitoring with wealth manager; dedicated relationship manager with verbal

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY	
					authentication protocol; regular review of authorized signers and beneficiaries
4	**Personal device security & patching**	**Keep them out**	Enable automatic updates on all personal devices including smartphones, tablets, laptops, and home network equipment (routers, access points, smart home devices). Use only supported operating systems—devices that no longer receive security updates should be replaced. Install a reputable endpoint protection solution/anti-virus on personal computers. Enable the native device encryption (e.g., BitLocker, FileVault) and remote wipe capability on mobile devices. Personal devices are increasingly targeted because they often lack the protections found in corporate environments yet may contain or provide access to sensitive information.	☐ **Partial**	Automatic updates disabled or ignored; devices running unsupported operating systems; no endpoint protection; no device encryption
				☐ **Risk-Informed**	Automatic updates enabled on primary devices; endpoint protection on laptop; some devices still on unsupported OS; encryption not consistently enabled
				☐ **Repeatable**	All devices on supported operating systems with automatic updates enabled; endpoint protection on all computers; device encryption enabled; remote wipe configured on mobile devices
				☐ **Adaptive**	All devices patched within days of release; firmware updates applied to home network equipment on a regular cadence; device inventory maintained; old devices securely wiped before disposal; family members' devices included in patching practices
5	**Secure Communications & Privacy**	**Keep them out**	Use end-to-end encrypted messaging for sensitive personal and financial communications. Avoid transmitting sensitive information—account numbers, Social Security numbers, tax documents—over unencrypted email or SMS. Use a VPN on public Wi-Fi networks on both your phone and laptop. Be	☐ **Partial**	Sensitive information shared over unencrypted email or SMS; no VPN; no awareness of voice deepfake threats
				☐ **Risk-Informed**	Encrypted messaging used occasionally; VPN available but not consistently used on public networks; some awareness of social engineering
				☐ **Repeatable**	End-to-end encrypted messaging used for all sensitive communications;

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY	
			cautious of unsolicited calls or messages requesting personal information, even if the caller appears to be from a known institution—callback using a verified number. High-profile individuals are increasingly targeted by voice deepfakes and social engineering impersonating trusted contacts or institutions.		VPN used on all public networks; sensitive documents shared only through secure channels; callback verification practiced for unsolicited requests
				☐ **Adaptive**	Family-wide encrypted communication practices; proactive awareness of deepfake voice/video impersonation; secure file sharing for all financial and legal documents; regular review of communication practices with advisors and household staff
6	**Home Network Security**	**Keep them out**	Change default passwords on all home network equipment (routers, access points, smart home devices). Use WPA3 encryption on Wi-Fi networks. Create a separate guest network for visitors and IoT devices (e.g. Smart TVs, smart thermostats, etc.). Disable remote management features unless specifically needed. Keep router and access point firmware updated. Your home network is the gateway to every connected device in your household—if it is compromised, attackers can intercept traffic, access personal devices, and pivot to corporate VPN connections.	☐ **Partial**	Default router credentials unchanged; no guest network; firmware never updated; WPA2 or older encryption
				☐ **Risk-Informed**	Router password changed; WPA2 or WPA3 in use; no guest network; firmware updates infrequent
				☐ **Repeatable**	WPA3 enabled; unique strong passwords on all network equipment; guest network for visitors and IoT devices; firmware updated regularly; remote management disabled
				☐ **Adaptive**	Network segmentation for IoT, guest, and personal devices; DNS-level filtering for malicious domains; network activity monitored for anomalies; professional security review of home network annually
7	**Social Media & Digital Footprint Management**	**Keep them out**	Review privacy settings on all social media accounts and limit publicly visible personal information—especially location data, travel plans,	☐ **Partial**	Social media profiles fully public; security question answers easily discoverable online; no awareness of digital footprint exposure

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY	
			family details, and financial affiliations. Avoid posting information that could be used to answer security questions or facilitate social engineering (e.g., pet names, schools, hometown). Periodically search for yourself online to identify exposed personal data or subscribe to a service that does this on your behalf (digital footprint management services). Attackers use publicly available information to craft targeted phishing, impersonation, and social engineering attacks.	☐ **Risk-Informed**	Some privacy settings tightened; aware of digital exposure but no proactive management; security questions not reviewed
				☐ **Repeatable**	Privacy settings reviewed and tightened on all platforms; location sharing disabled; security questions use non-guessable answers; periodic self-search conducted; data broker opt-outs completed
				☐ **Adaptive**	Professional digital footprint management service engaged; continuous monitoring for personal data exposure; family members included in digital footprint practices; social media activity reviewed for operational security risks
8	**Personal Cyber & Fraud Insurance**	**Limit the damage**	Review your homeowner's insurance policy and add cyber insurance coverage. Many standard policies exclude or severely limit cyber and fraud losses. If your insurance carrier does not provide, you may need to consider moving to an insurer that offers the coverage. Coordinate personal coverage with your business cyber policy to avoid gaps. Review annually with your insurance agent. If you do not know whether your personal losses from a cyber event are covered, assume they are not.	☐ **Partial**	No awareness of personal cyber coverage; relying on standard homeowner's policy; no review with agent
				☐ **Risk-Informed**	Aware of coverage gaps; homeowner's policy reviewed for cyber exclusions; no personal cyber coverage endorsement on homeowner’s policy
				☐ **Repeatable**	Personal cyber insurance in place covering identity theft, financial fraud, cyber extortion, and incident response; annual review with insurance agent; personal and business coverage coordinated
				☐ **Adaptive**	Comprehensive personal cyber policy with higher limits; coverage tested against realistic loss scenarios; annual tabletop or review with family office, agent, and counsel; coverage

#	CONTROL	FUNCTION	WHAT GOOD LOOKS LIKE	YOUR PERSONAL CYBER MATURITY
				adjusted as threat landscape evolves