Data-Protection Kit (2025)

Purpose

Regulatory change, ransomware campaigns and new adversaries mean organisations must review how they classify and protect their data. Recent analysis shows the average ransomware payout has risen to roughly **$1 million** and recovery costs can reach **$1.5 million** in 2025, while 75 % of organisations experienced at least one ransomware attack last year. Critical sectors such as healthcare recorded **458 ransomware incidents** in 2024, and PRC-linked espionage campaigns have targeted telecommunications providers. Meanwhile, U.S. state privacy laws are accelerating: five new state privacy laws took effect on 1 January 2025 and three more will activate later in the year. This kit helps you quickly identify which data categories your organisation handles and provides tailored controls, checklists and templates to mitigate associated threats.

Step 1 – Classify your high-value data

Use the table and questions below to classify the data you process. Organisations often manage multiple categories.

Data categories and typical examples

Category	What it includes	Key drivers
Payment & PII	Cardholder data (credit/debit cards), personal identifiers (names, addresses, email/phone numbers, government IDs), financial account details. PII can be direct (e.g., passport number) or indirect (e.g., IP address, date of birth).	Highly regulated (PCI DSS, GDPR, state privacy laws). Attractive for fraud and identity theft.
Healthcare/Biometrics	Protected health information (PHI), medical device telemetry, lab results, genomic/biometric identifiers. New state privacy laws classify children's data and biometric data as sensitive.	Strict laws (HIPAA, state laws) and high ransom values. In 2024 the health sector suffered 458 ransomware events.
Telecom/Infra Ops	Call-detail records, network configuration files, signalling logs, core routing/switch software, outage reports,	Nation-state espionage; PRC-affiliated actors compromised major telecom networks and defenders are

Category	What it includes	Key drivers
	credentials.	urged to strengthen visibility and patching.
Industrial/OT	Industrial control system (ICS) configurations, programmable logic controller (PLC) code, SCADA data, plant process set-points, safety override settings.	Disruption can have physical consequences; new guidance urges organisations to maintain a definitive OT asset inventory and align with IEC 62443/ISO 27001.
Crypto/Fintech	Digital asset wallets, private keys, seed phrases, exchange/API credentials, transaction records, trading algorithms. Cybercrime targeting cryptocurrency surged 600 % in early 2023 before easing.	High-value theft targets; sensitive to phishing and malware.
IP/R&D	Source code, CAD/engineering files, proprietary formulas, AI models, trade secrets and confidential compilations of data. Courts recognise broad forms of information as trade secrets if reasonable measures keep them secret.	Competitive advantage; nation-state espionage and insider theft.

Quick classification questions

Answer **yes** or **no** for each question. Assign the data sets where you answered “yes” to the corresponding category.

1. **Do you process payments or store personally identifiable information (PII)?** This includes card numbers, full names, addresses, contact details, government IDs, financial accounts or other identifiers.
2. **Do you handle protected health information or biometric identifiers?** If you process medical records, patient data, clinical research, genomics or device telemetry, mark *Healthcare/Biometrics*. State privacy laws classify children’s data and genetic/biometric data as sensitive.
3. **Are you responsible for telecommunications or critical network operations?** If you run cell towers, network management systems, signalling data, call-detail logs or base station software, mark *Telecom/Infra Ops*.

4. **Do you operate industrial control systems or manage plant-level operational technology (OT)?** If you run manufacturing lines, power grids, transport systems or similar physical processes, mark *Industrial/OT*.
5. **Do you manage digital assets or financial technology?** If you hold cryptocurrency wallets, private keys, API keys, trading data or run fintech services, mark *Crypto/Fintech*.
6. **Do you hold proprietary designs, source code, R&D data or other trade secrets?** If yes, mark *IP/R&D*. Trade secrets can include compilations of financial or customer data when the organisation takes reasonable steps to keep them secret.

Record your answers in the **Data Inventory Template** below.

Data inventory template

Data set name	Category	Owner & stakeholders	Storage locations (cloud/on-prem)	Access paths (e.g., SaaS, VPN, API)	Regulatory obligations
Example: Customer billing info	Payment & PII	Finance & IT	CRM (SaaS), ERP (on-prem)	Web portal; API for billing	PCI DSS; GDPR; local privacy laws
Your data set					

Populate the table for your top five data sets. Use this inventory to prioritise controls.

Step 2 – Understand the threat landscape

After classification, map each category to likely adversaries and motivations. The table below summarises typical attackers and goals. It is based on recent threat intelligence, including the 2025 Health-ISAC report and CISA guidance.

Category	Likely adversaries	Motivations & observed tactics
Payment & PII	Organised crime groups, initial-access brokers, ransomware-as-a-service (RaaS) crews	Rapid monetisation via credit-card fraud, identity theft and extortion. PII is valuable because it enables account takeover and phishing campaigns. Attackers often use phishing, info-stealer malware and credential stuffing to breach cardholder data and may sell access to ransomware

Category	Likely adversaries	Motivations & observed tactics
		gangs.
Healthcare/Biometrics	Nation-state espionage units, sophisticated crime syndicates, RaaS affiliates (e.g., LockBit 3.0, BianLian, INC Ransomware)	Steal sensitive health data for intelligence or ransom. The Health-ISAC tracked **458 ransomware events** against healthcare in 2024. Groups like **BianLian** use living-off-the-land tools and fast encryptors, while **INC Ransomware** uses spear-phishing and legitimate Windows tools such as WordPad and Paint to evade detection. Nation-state actors such as **APT29** exploit VPN vulnerabilities and conduct supply-chain attacks for espionage.
Telecom/Infra Ops	Nation-state actors (PRC-affiliated, other espionage groups), advanced persistent threat (APT) groups	Strategic access and espionage. CISA notes that PRC-linked actors compromised global telecom networks and emphasises that patching vulnerable devices and securing environments reduce opportunities for intrusion. Attackers may abuse default credentials, outdated firmware, and misconfigured remote management.
Industrial/OT	Nation-states (targeting critical infrastructure), hacktivists, ransomware crews	Disruption, sabotage and extortion. Modern OT is tightly integrated with IT networks; guidance from CISA/NCSC stresses the need to build a definitive OT asset inventory and align with standards like **IEC 62443** and **ISO/IEC 27001**. Threat actors exploit remote access and supply-chain vulnerabilities to stage wiper attacks, lateral movement and ransomware.

Category	Likely adversaries	Motivations & observed tactics
Crypto/Fintech	Organised crime syndicates, crypto-native hacking crews, phishing and malware operators	Theft and laundering of digital assets. Cybercrime targeting cryptocurrency spiked **600 %** in early 2023. Attacks focus on stealing private keys or seed phrases via phishing, infostealers or exploitation of browser extensions. Rug pulls and API key theft are common.
IP/R&D	Nation-state espionage units, competitors, insider threats	Economic advantage. Remote work and easy digital transfer increase misappropriation risk. Some adversaries, including North Korean operatives, masquerade as remote IT workers to steal IP and money. Attackers may use phishing, supply-chain compromise, or recruit insiders.

Step 3 – Use the kit's tools

This kit provides three self-service tools to get started:

1. Data inventory & classification worksheet

Use the template above to list each data set, assign a category, note storage locations and interfaces, and identify regulatory obligations. Completing this inventory enables targeted protection and regulatory compliance.

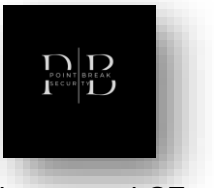
2. Category questionnaire

For each data set, answer the classification questions. For example, if you process cardholder data and PII, mark "Payment & PII". If you store genomic data or biometric identifiers, mark "Healthcare/Biometrics". Some data sets may fall into multiple categories (e.g., medical billing records combine Payment & PII and Healthcare/Biometrics). Assign all applicable categories.

3. Threat mapping & risk scoring

For each data set, map the adversary column(s) from Step 2. Consider: who would most benefit from attacking this data? Use a simple **High/Medium/Low** rating for:

- **Attractiveness** – Would criminals quickly monetise this data? Payment and crypto keys are usually high.



- **Impact** – If compromised, would it disrupt life-critical services? Healthcare and OT are high because attacks can harm patients or physical processes.
- **Regulatory exposure** – Are there significant fines for breaches? PII and healthcare data face HIPAA/GDPR penalties and new state privacy laws.

Prioritise controls on assets that score high across these dimensions.

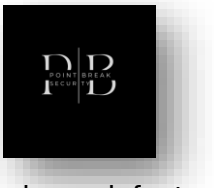
Step 4 – Apply category-specific control checklists

Payment & PII

- **Implement phishing-resistant multi-factor authentication (MFA)**: The latest PCI DSS v4.0 mandates MFA for any access to cardholder data environments, reflecting its importance for payment security. Enforce strong MFA across all systems storing PII and disable legacy/weak authentication.
- **Maintain an up-to-date inventory of cryptographic keys and certificates**: PCI DSS 4.0 requires organisations to identify and inventory all cryptographic assets and ensure strong algorithms.
- **Encrypt PII at rest and in transit** using modern encryption, and avoid storing full card data unless strictly necessary. State privacy laws require limiting collection and processing of sensitive data to what is strictly necessary.
- **Minimise data collection**: Review forms and logs to ensure that you only collect data relevant to your service. New laws such as Maryland's 2025 privacy act ban the sale of sensitive personal data and broaden "sensitive" to include consumer health, national origin, and biometric information.
- **Implement skimming detection for e-commerce**: PCI DSS 4.0 introduces new requirements to detect web-skimming and prevent tampering. Use content security policies and integrity checks.
- **Monitor for credential stuffing and info-stealer logs**: Keep an eye on underground markets and implement account-takeover detection; enforce passwordless or passkey-based authentication where possible.

Healthcare/Biometrics

- **Conduct regular risk assessments and engage stakeholders**: Healthcare breaches cost an average of $9.77 million per incident in 2024, so prioritise identifying vulnerabilities.
- **Adopt Zero-Trust access controls**: Use role-based authentication and continuous identity verification for clinicians, vendors and service accounts. MFA should be phishing-resistant.
- **Encrypt and back up patient data**: Maintain immutable, off-line backups to restore services quickly after ransomware.
- **Continuously monitor networks and medical devices**: Implement real-time monitoring and threat intelligence to detect living-off-the-land attacks.



Ransomware gangs such as BianLian leverage native Windows tools and fast encryptors; detection must focus on anomalous use of built-in binaries.

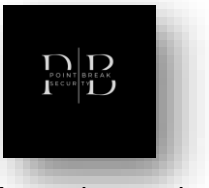
- **Review supply-chain and vendor risk**: Nation-state actors like APT29 exploit VPN vulnerabilities and supply-chain software. Ensure vendors patch remote access software promptly and comply with security requirements.
- **Vet remote employees and contractors**: Health-ISAC reports that North Korean operatives are masquerading as remote IT workers to steal intellectual property and extort organisations. Use identity verification, background checks and device posture controls.

Telecom/Infra Ops

- **Harden network infrastructure**: Patch routers and switches promptly. The enhanced visibility guidance stresses that patching vulnerable devices and services reduces opportunities for intrusion.
- **Encrypt configuration transfers**: Send network configurations using encrypted protocols (SSH, SFTP). Avoid emailing plaintext configs or using FTP/TFTP.
- **Establish change and patch management**: Monitor vendor end-of-life announcements and apply patches promptly. Use a change management system that anticipates routine and emergency patching.
- **Require phishing-resistant MFA for all administrative accounts** and enforce session expirations. Use a central AAA server and limit local accounts to emergency use.
- **Implement RBAC and least-privilege**: Assign users only the permissions needed to perform their tasks.
- **Disable unused services**: Follow vendor-specific hardening guides (e.g., disable Cisco Smart Install, telnet and non-encrypted web management).
- **Incident reporting**: Know how to report suspicious activity to authorities and cross-border partners.

Industrial/OT

- **Create a definitive OT asset inventory**: New 2025 guidance from CISA and the UK NCSC emphasises building an up-to-date “definitive record” of OT assets using asset inventories and vendor-provided software bills of materials. This record enables holistic risk assessments and targeted protections.
- **Collaborate across IT and OT teams**: OT security requires coordination between engineers and IT. The guidance recommends cross-team collaboration and alignment with international standards like **IEC 62443** and **ISO 27001**.
- **Segment networks and secure remote access**: Ensure that OT systems are isolated from corporate IT networks whenever possible. Use dedicated gateways and multi-factor authentication for remote connections. Monitor for lateral movement via VPN vulnerabilities.



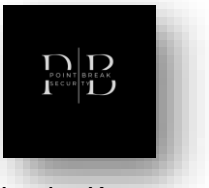
- **Apply patch management carefully**: Many OT devices have long life cycles and limited patch windows; track vendor advisories and schedule downtime for updates.
- **Develop incident response plans** that address physical safety and environmental impact in addition to data integrity. Practice tabletop exercises.

Crypto/Fintech

- **Use cold wallets for long-term storage**: Keep private keys offline to protect against malware and network-based theft. Cold storage reduces exposure to hackers.
- **Back up wallet data in multiple secure locations**: Store backups offline and encrypt them. Protect seed phrases using secure storage (metal plates or offline vaults).
- **Enable multi-signature wallets**: Require multiple approvals for transactions. Multisig wallets add an extra layer of security and prevent a single compromised key from draining funds.
- **Use strong, unique passwords and two-factor authentication**: 2FA and complex passwords reduce account takeover. Avoid reusing passwords and consider passwordless passkeys.
- **Regularly update wallet software and firmware** to address vulnerabilities.
- **Distribute assets across multiple wallets**: Spreading funds minimises impact if a single wallet is compromised.
- **Beware of phishing and malicious browser extensions**: Attackers often impersonate crypto services or inject “clippers” to steal addresses. Educate employees and implement browser isolation for high-value operations.

IP/R&D

- **Define and document your trade secrets**: Under the Defend Trade Secrets Act, information qualifies as a trade secret when it is secret, valuable and subject to reasonable measures to maintain secrecy. Identify and label such data.
- **Restrict access and implement confidentiality policies**: Courts recognise measures such as clear confidentiality policies, NDAs for employees and contractors, physical security for sensitive areas, and digital controls (access control, encryption, monitoring) as reasonable. Use data-loss prevention (DLP) tools and file-level encryption.
- **Train employees and manage onboarding/offboarding**: Regularly train staff on handling confidential information and ensure departing employees return all proprietary data.
- **Monitor for unusual exfiltration**: Use security analytics to detect large uploads or unusual repository activity. Monitor code repositories and design tools for access anomalies.



- **Vet remote workers and suppliers**: Health-ISAC notes that North Korean operatives pose as remote IT contractors to steal IP and extort organisations. Implement pre-employment screening and device compliance checks.
- **Develop an incident response plan for trade secret theft**: Prepare legal and technical steps to investigate and seek injunctions. Document evidence of reasonable measures; courts look for these when awarding damages.

Step 5 – Cross-cutting controls

Many controls apply across all categories:

- **Identity & access management**: Deploy phishing-resistant MFA on all administrative accounts and critical applications. Limit account privileges using RBAC and review accounts regularly.
- **Patch & configuration management**: Maintain an accurate inventory of hardware and software. Monitor for EOL announcements and apply security patches promptly. In OT environments, coordinate with operational teams and schedule downtime appropriately.
- **Network segmentation & zero trust**: Separate sensitive data and OT networks from corporate IT. Use micro-segmentation and network access controls. For telecom and OT, disable unneeded services and enforce encrypted management protocols.
- **Backup & incident response**: Maintain immutable, offline backups and test restoration. Develop playbooks for ransomware, data theft and insider threats. Include procedures for contacting law enforcement and regulators.
- **Supply-chain risk management**: Vet suppliers and partners for security practices. Require SaaS and MSPs to support SSO, SCIM provisioning, device posture checks and logging. Monitor for exploitation of third-party VPN or remote management tools.
- **Privacy & regulatory compliance**: Stay abreast of new privacy laws. The 2025 U.S. state privacy laws impose strict limits on collecting and selling sensitive data, require universal opt-out mechanisms and may obligate organisations to name a Chief Privacy Officer. Adopt frameworks such as NIST Privacy Framework to qualify for affirmative defence provisions in some states.
- **AI & generative AI governance**: Many breaches now involve AI-generated phishing and deepfakes. Establish policies governing AI usage, restrict unsanctioned AI tools, and monitor for unverified OAuth applications.