Data protection

January 2019

ACCION

Investing in individuals.
Improving our world.

Data Protection includes both Privacy and Security

Data Privacy

- Do our customers **understand and agree to** what data is captured and how it's used?
- **Who owns** our customer data – who can change/erase it?

- How should we manage data integrations with our **partners**?
- What **regulatory & compliance** issues must we manage?
- How can we **move our organization** toward greater privacy & security?
- What is the best **response** to a breach?

Data Security

- What **infrastructure solutions** do we need to protect against breaches?
- What **technical solutions** do we need to protect against breaches?
- What **processes** should we implement to ensure security?
- How do we **stay up to date** with security challenges?

Significant areas of overlap – important to consider privacy and security topics jointly

ACCION

The right data protection mindset – technology and people

	Capture	Transport	Store	Access	Use	Share
Technical precautions	• Secure data capture	• Encryption & decryption practices	• Encryption at-rest • Network security	• Tiered access limits	• Internal application security	• 3rd-party integrations and service-level agreements
Human precautions	• Transparency and consent for customers	• File sharing methods • Laptop locking	• File retention practices	• Locks on server room doors • Password reset	• Usage limitations for sensitive data	• Process to bring on new vendors

Both technical and "human" precautions are needed for each stage of the "data lifecycle"

ACCION

Why care about data protection?

Maintain your customers' trust

Customers care about this, and it must be part of your brand

Avoid legal and regulatory problems

Fines, lawyers, and distraction use valuable time and money

Keep your company running

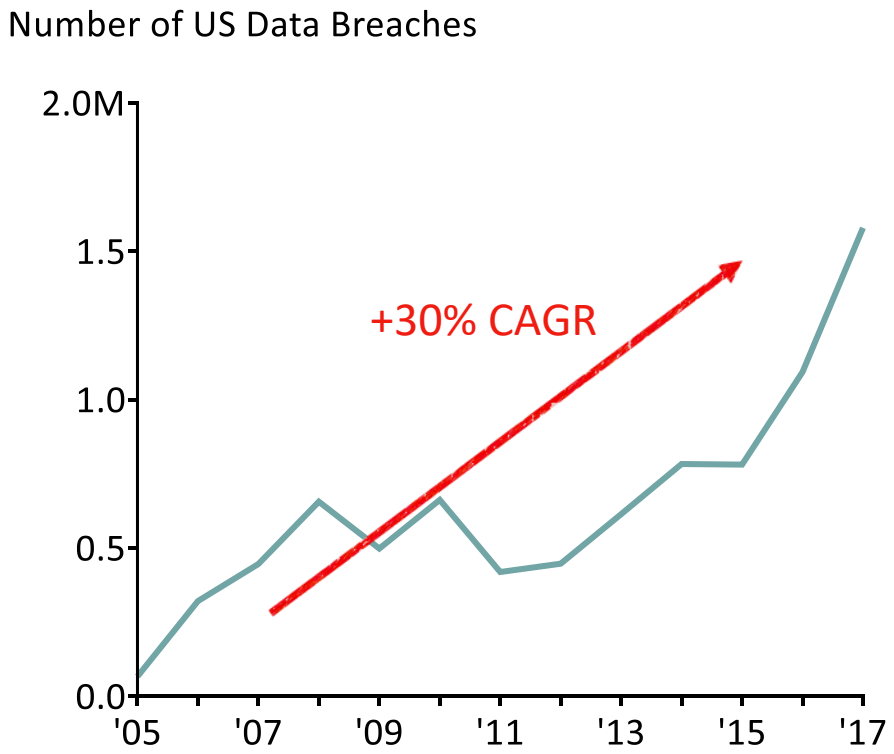
Outages can kill momentum and stop you from gaining traction

55% of customers at risk of leaving in case of a breach

66 days average time to contain a data breach once identified

Sources: Customer Trust, Data breach

The right data protection mindset – evolve with the times



Hackers are increasingly **prevalent and sophisticated**

Regulators are increasing scrutiny of businesses

Business leaders must constantly stay on top of data protection issues

ACCION

The right data protection mindset – make the right tradeoffs

Risk increases with the **volume and value** of your data.

Financial services companies are at higher risk of attack

Risk of data protection issue

Startup

"Nobody cares enough about our 10 customers to cause an issue – growth is more important than perfect security"

Growth

"Still early enough that recovery from a major data issue would be difficult, but we're under the radar enough that we're facing few direct attacks"

Established

TARGET EQUIFAX

"People know that we have sensitive data, so are actively attacking us from multiple angles"

High-profile

"Every blackmailer, state actor, and class action lawyer wants a piece of us"

Time and money spent on data protection

The "right" security approach is one appropriate for your business' size, stage, and data sensitivity; however, it is important to consider the tradeoff of building security right the first time vs. retrofitting at a later stage

ACCION

First step to improve data protection: discovery

	Discovery	Design	Implementation
Questions to answer	• What level of data protection is appropriate for our data? • What gaps do we have in our current level of data protection?	• Where do I need to get to on data protection? • What initiatives do I need to put in place to get there?	• How should I roll out changes to data protection in my company? • How can investors test & support pre- and post-investment?
Resources in this guide	• Data audit and risk assessment workshop templates  • Data protection assessment 	• Targeted content on key topics  • Data policy template  • Initiative list template 	• Initiative prioritization template  • Implementation checklist  • Investor diligence & portfolio management guide 
	Click HERE for data protection assessment	Click HERE for data policy template	See appendix of resource for all other blank templates

ACCION

Various ways to do Discovery – choose what fits best

		What it looks like	Cost*	Appropriate if…
Partially Dedicated	**Existing Team**	• Executive leaders run discovery, design, implementation • Some outsourced security testing (penetration testing)	 ($5-12K black box/ $40-100K white box)	• Angel / Seed • Experienced technology team • Available management bandwidth to lead process and cultural changes
	Virtual CISO *(on contract for full year)*	• Senior leader hired to do discovery and design • Accountability sits with them, but not full-time or on-site	 ($30-60K)	• Seed / Series A • Experienced technology team • Low management bandwidth to lead process and cultural changes
Fully Dedicated	**Consultant** *(assuming a 4 month project)*	• Third-party runs discovery process & facilitates design • Implementation handled by internal team	 ($50-100K)	• Seed / Series A • Inexperienced technology team • Low management bandwidth to lead process and cultural changes
	Full-time CISO	• Senior leader hired to oversee all data protection – discovery, design, implementation, monitoring, etc.	 ($100-250K)	• Series A / B • Sufficient funding to pay for role • Evidence of persistent threats

*Calculated for companies located in the US

ACCION

Two parts to the discovery process

1 Data audit and strategy

- Understand your **data landscape**
  - What data is captured
  - Who owns and can access the data
  - How the data is used
- Assess **importance of data protection** for each data element
- Determine **level of risk you're comfortable with** for various data elements

2 Data protection assessment

- **Assess where you stand** on key data protection topics
  - Data privacy
  - Partner management
  - Technical security – software, infrastructure
  - Data management
  - Culture
  - Breach response

ACCION

1 Discovery: data protection workshop template

What is our data landscape?

Data	Data type	Location	Owner	How used	Who can access
Customer demographics	• Customer	• Internal	• CMO	• Credit scoring • KYC • Customer service	• Customer service reps • Credit team • Etc.
Credit scores	• Business	• Cloud	• CRO	• Underwriting	• Credit team • Management

ACCION

1 Discovery: data protection workshop template

How essential is data protection for each of our data elements?

	Internal data	External data
Significant regulation	• …	• …
Other business critical	• …	• …
Other data	• …	• …

EXAMPLE DATA ELEMENTS

- Customer demographics
- Payment history
- Payment cards
- Credit history
- Internal scoring
- Employee demographics

ACCION

1 Discovery: data protection workshop template

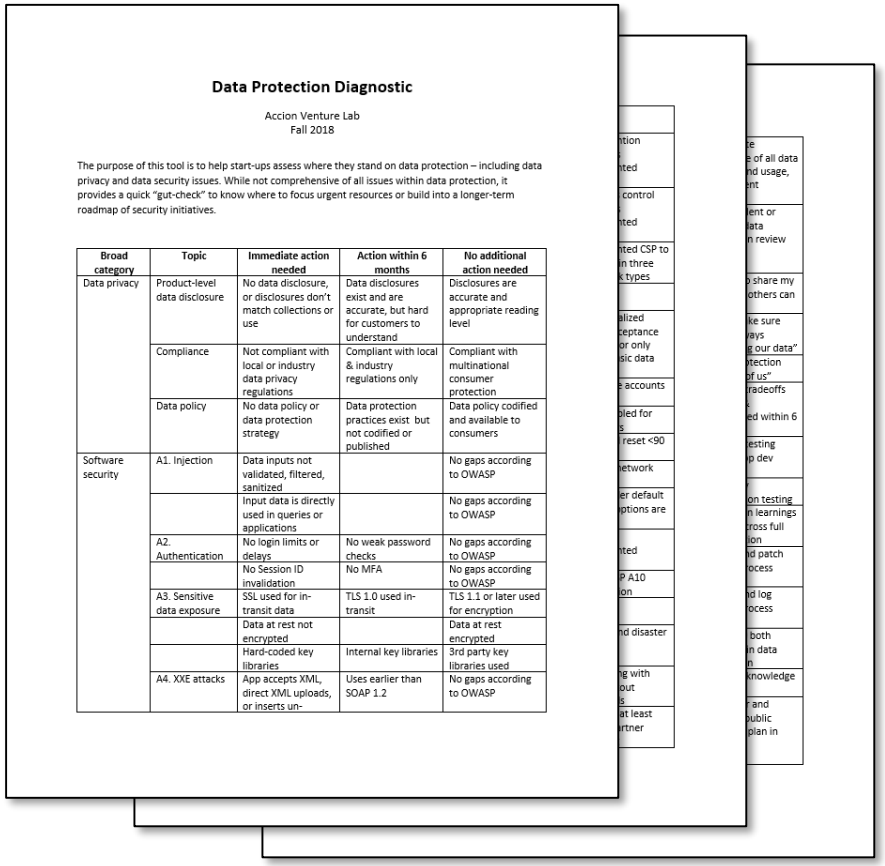
Based on the previous two pages, what risk are we comfortable with on each type of data?

Data	Risk tolerance	Rationale
Customer data	Zero	• Our business depends on consumer confidence, and misuse or compromise of customer data would cause significant damage to the business
Internal messaging	Low	• Internal communications may contain sensitive content which shouldn't fall into hands of competitors or potentially cause bad press. However, we recognize that some level of sharing is inevitable

2 Discovery: data protection assessment

We've created a "stoplight" assessment for you to quickly check where you stand (link here)

- Data privacy
- Partner management
- Technical security – software, infrastructure
- Data management
- Culture
- Breach response



Data Protection Diagnostic

Accion Venture Lab
Fall 2018

The purpose of this tool is to help start-ups assess where they stand on data protection – including data privacy and data security issues. While not comprehensive of all issues within data protection, it provides a quick "gut-check" to know where to focus urgent resources or build into a longer-term roadmap of security initiatives.

Broad category	Topic	Immediate action needed	Action within 6 months	No additional action needed
Data privacy	Product-level data disclosure	No data disclosure, or disclosures don't match collections or use	Data disclosures exist and are accurate, but hard for customers to understand	Disclosures are accurate and appropriate reading level
	Compliance	Not compliant with local or industry data privacy regulations	Compliant with local & industry regulations only	Compliant with multinational consumer protection
	Data policy	No data policy or data protection strategy	Data protection practices exist but not codified or published	Data policy codified and available to consumers
Software security	A1. Injection	Data inputs not validated, filtered, sanitized		No gaps according to OWASP
		Input data is directly used in queries or applications		No gaps according to OWASP
	A2. Authentication	No login limits or delays	No weak password checks	No gaps according to OWASP
		No Session ID invalidation	No MFA	No gaps according to OWASP
	A3. Sensitive data exposure	SSL used for in-transit data	TLS 1.0 used in-transit	TLS 1.1 or later used for encryption
		Data at rest not encrypted		Data at rest encrypted
		Hard-coded key libraries	Internal key libraries	3rd party key libraries used
	A4. XXE attacks	App accepts XML, direct XML uploads, or inserts un-	Uses earlier than SOAP 1.2	No gaps according to OWASP

ACCION

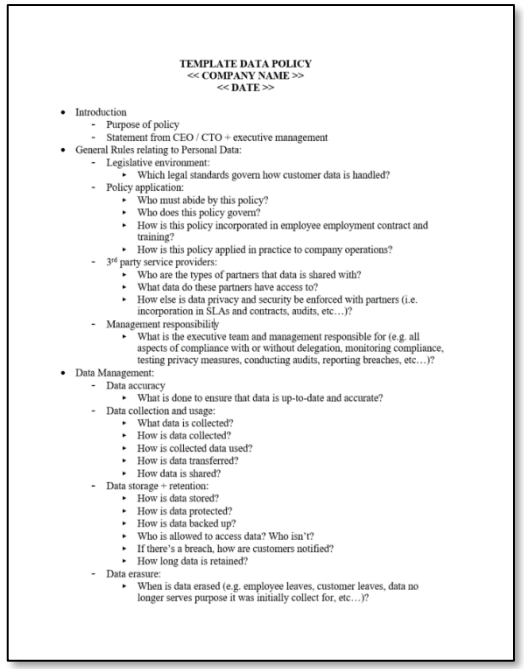
Second step to improve data protection: design

	Discovery	Design	Implementation
Questions to answer	• What level of data protection is appropriate for our data? • What gaps do we have in our current level of data protection?	• Where do I need to get to on data protection? • What initiatives do I need to put in place to get there?	• How should I roll out changes to data protection in my company? • How can investors test & support pre- and post-investment?
Resources in this guide	• Data audit and risk assessment workshop templates  • Data protection assessment 	• Targeted content on key topics  • Data policy template  • Initiative list template 	• Initiative prioritization template  • Implementation checklist  • Investor diligence & portfolio management guide 
	[Click HERE for data protection assessment]	[Click HERE for data policy template]	[See appendix of resource for all other blank templates]

ACCION

Design: should produce two key outputs

INITIAL DRAFT OF DATA POLICY



TEMPLATE DATA POLICY
<< COMPANY NAME >>
<< DATE >>

- Introduction
  - Purpose of policy
  - Statement from CEO / CTO + executive management
- General Rules relating to Personal Data:
  - Legislative environment:
    - Which legal standards govern how customer data is handled?
  - Policy application:
    - Who must abide by this policy?
    - Who does this policy govern?
    - How is this policy incorporated in employee employment contract and training?
    - How is this policy applied in practice to company operations?
  - 3rd party service providers:
    - Who are the types of partners that data is shared with?
    - What data do these partners have access to?
    - How else is data privacy and security be enforced with partners (i.e. incorporation in SLAs and contracts, audits, etc…)?
  - Management responsibility
    - What is the executive team and management responsible for (e.g. all aspects of compliance with or without delegation, monitoring compliance, testing privacy measures, conducting audits, reporting breaches, etc…)?
- Data Management:
  - Data accuracy
    - What is done to ensure that data is up-to-date and accurate?
  - Data collection and usage:
    - What data is collected?
    - How is data collected?
    - How is collected data used?
    - How is data transferred?
    - How data is shared?
  - Data storage + retention:
    - How is data stored?
    - How is data protected?
    - How is data backed up?
    - Who is allowed to access data? Who isn't?
    - If there's a breach, how are customers notified?
    - How long data is retained?
  - Data erasure:
    - When is data erased (e.g. employee leaves, customer leaves, data no longer serves purpose it was initially collect for, etc…)?

12-MONTH CHANGE VISION

Other key changes not captured in the data policy

- Process adjustments
- Cultural shifts
- Structural changes

INITIATIVE LIST

Design: use policy & vision to create a list of initiatives

Initiative name *How you'll refer to the initiative*	Policy / Vision *"Future State" you're working toward*	How to get there *Specific changes to process or technology*
Example: Security code review	• All code reviewed for security before deployment	• Each developer has partner for security review • Managers send Slack message with "did you do your security review" to full team 12 hours before deploy. • Testing team implements new automatic security testing software to process
Example: Employee recognition	• Employees celebrated if they identify security risks	• Email recognition by accountable executive if employees identify phishing attack

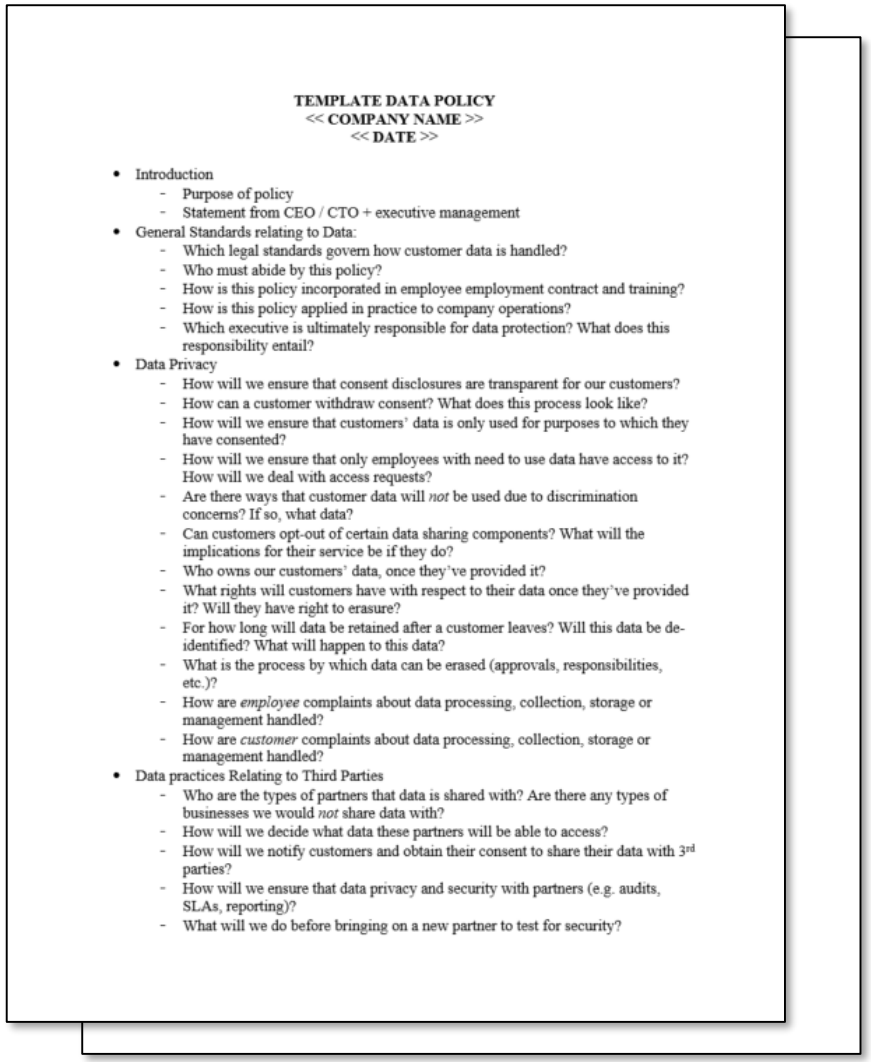
EXAMPLE

ACCION

You should review annually and consider refreshing your policy & processes

ACCION

Design: data policy



TEMPLATE DATA POLICY
<< COMPANY NAME >>
<< DATE >>

- Introduction
  - Purpose of policy
  - Statement from CEO / CTO + executive management
- General Standards relating to Data:
  - Which legal standards govern how customer data is handled?
  - Who must abide by this policy?
  - How is this policy incorporated in employee employment contract and training?
  - How is this policy applied in practice to company operations?
  - Which executive is ultimately responsible for data protection? What does this responsibility entail?
- Data Privacy
  - How will we ensure that consent disclosures are transparent for our customers?
  - How can a customer withdraw consent? What does this process look like?
  - How will we ensure that customers' data is only used for purposes to which they have consented?
  - How will we ensure that only employees with need to use data have access to it? How will we deal with access requests?
  - Are there ways that customer data will *not* be used due to discrimination concerns? If so, what data?
  - Can customers opt-out of certain data sharing components? What will the implications for their service be if they do?
  - Who owns our customers' data, once they've provided it?
  - What rights will customers have with respect to their data once they've provided it? Will they have right to erasure?
  - For how long will data be retained after a customer leaves? Will this data be de-identified? What will happen to this data?
  - What is the process by which data can be erased (approvals, responsibilities, etc.)?
  - How are *employee* complaints about data processing, collection, storage or management handled?
  - How are *customer* complaints about data processing, collection, storage or management handled?
- Data practices Relating to Third Parties
  - Who are the types of partners that data is shared with? Are there any types of businesses we would *not* share data with?
  - How will we decide what data these partners will be able to access?
  - How will we notify customers and obtain their consent to share their data with 3rd parties?
  - How will we ensure that data privacy and security with partners (e.g. audits, SLAs, reporting)?
  - What will we do before bringing on a new partner to test for security?

DATA POLICY TEMPLATE

- We have created a template for companies to use while drafting an initial data policy

- The template covers **three major sections**:
  - General Rules
  - Data Management
  - Breach Response

- Within each section, you will be **guided by specific questions** to better understand what information should fall within each section

- The template is now available as a **resource on our website** here

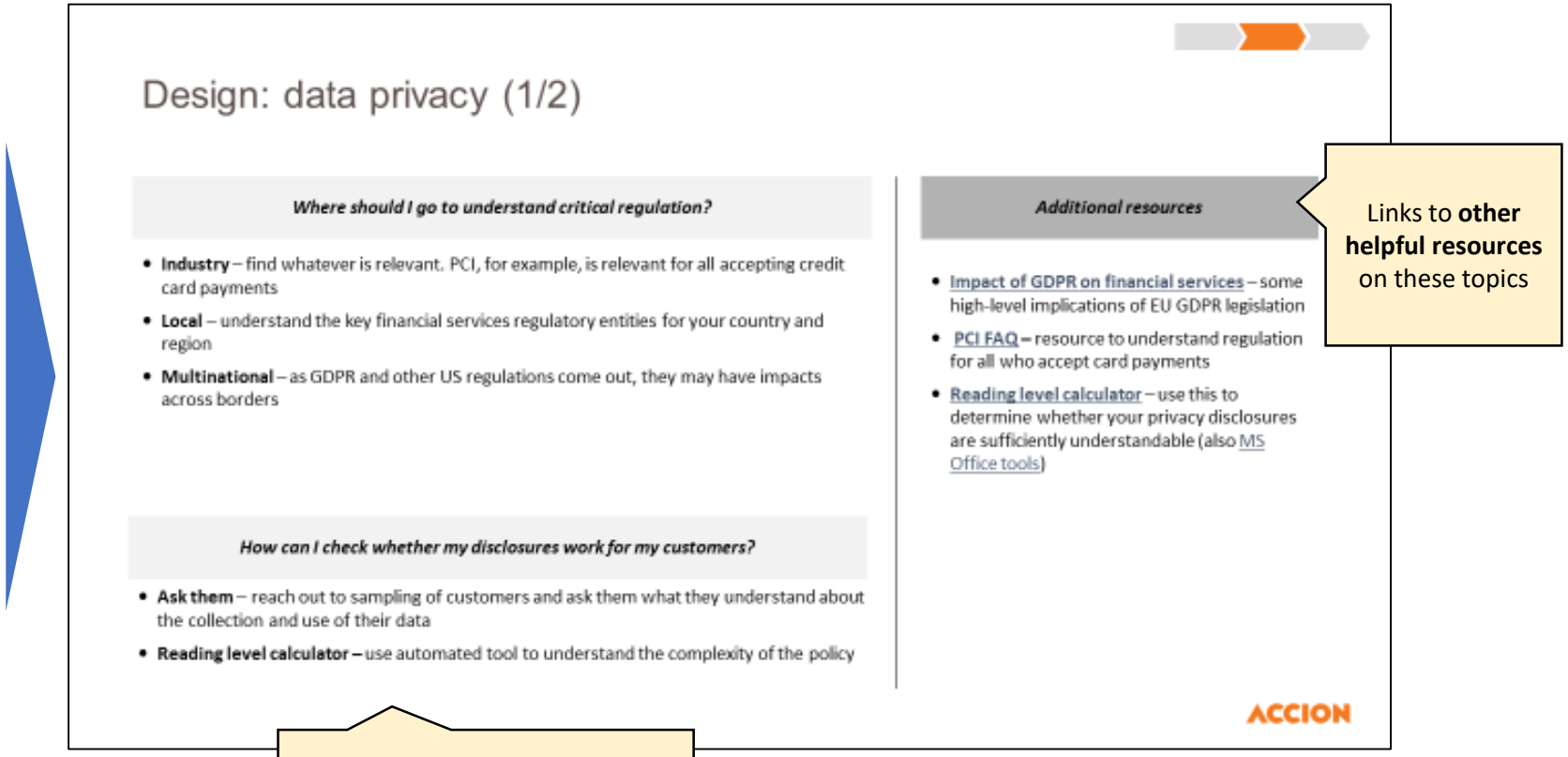
Design: use policy and vision to create a list of initiatives

Initiative name *How you'll refer to the initiative*	**Policy / Vision** *"Future State" you're working toward*	**How to get there** *Specific changes to process or technology*
Example: Security code review	• All code reviewed for security before deployment	• Each developer has partner for security review • Managers send Slack message with "did you do your security review" to full team 12 hours before deploy. • Testing team implements new automatic security testing software to process
Example: Employee recognition	• Employees celebrated if they identify security risks	• Email recognition by accountable executive if employees identify phishing attack

Design: this guide provides guidance to create policy and vision

For each component of data protection, we've identified key questions and resources

- Data privacy
- Partner management
- Technical security – software, infrastructure
- Data management
- Culture
- Breach response



Links to **other helpful resources** on these topics

Key questions and summarized insights – based on feedback from experts and startup teams

ACCION

Design: data privacy (1/2)

Where should I go to understand critical regulation?

- **Industry** – find whatever is relevant. PCI, for example, is relevant for all accepting credit card payments
- **Local** – understand the key financial services regulatory entities for your country and region
- **Multinational** – as GDPR and other US regulations come out, they may have impacts across borders

How can I check whether my disclosures work for my customers?

- **Ask them** – reach out to sampling of customers and ask them what they understand about the collection and use of their data
- **Reading level calculator –** use automated tool to understand the complexity of the policy

Additional resources

- Impact of GDPR on financial services – some high-level implications of EU GDPR legislation
- PCI FAQ **–** resource to understand regulation for all who accept card payments
- Reading level calculator – use this to determine whether your privacy disclosures are sufficiently understandable (also MS Office tools)

ACCION

Design: data privacy (2/2)

What does "good" look like when it comes to data privacy?

Overall Best Practices	Capture	Usage	Retention & Erasure
Be extremely transparent Customers don't typically understand (or read) disclosures – so don't assume that they do!	• *Always obtain consent to access and use customer data* – include what data, how it'll be used, and any other key legal • *When obtaining consent, think of the customer* – easy to read, jargon-free, mobile friendly, local language, etc. Use key facts statements.	• *Share how providing data helps the customer* – e.g. "Your location data lets us 1) verify your identify to give you better rates, as well as provide tailored marketing to you…" • *High-level and detailed versions* – full legal consent may include more detail	• *Tell customers what data will be retained, for how long, and in what form:* - De-identified vs. identified - Single data pull vs. ongoing feed - Physical vs. electronic
Keep all data confidential Especially with personal data, maintaining confidentiality preserves trust	• *Check customer disclosures of data acquired from partners* – even being one level removed carries some risk • *Highlight confidentiality when acquiring data* • *Be particularly careful with identity*	• *Proactively notify customers when sharing their data with 3rd parties* – e.g. bureaus, partners • *Only use the data for its intended purpose* – tier access and permissions, process checks if data used inappropriately	• *Upon erasure, ensure data is completely deleted across where it's stored* – incl. with partners, redundant servers, etc.
Let customers "own" their data Whether or not this is legally the case in your geography, that's likely what customers think. To maintain their trust, act as if their data is their own	• *Where possible, allow customers to opt-out of specific data access* – clearly explain consequences (e.g. higher prices, potential to not be approved)	• *Where possible, allow customers to opt-out of specific data uses* – for more intrusive data such as geolocation, restrictions on how that data may be used	• *Have a process for customers to request updates to, correction of, or erasure of their information* – self-service or through customer support • *Have a process to withdraw consent* – ensure clear explanation of the consequences of withdrawal
Take, keep, and use only what's valuable All data carries risk, so don't collect data for data's sake or keep data that is no longer relevant to your needs.	• *Don't collect all data for all customers* – identify the pieces which drive the most business value, and don't collect the rest	• *Be particularly conscious of regulation when using sensitive classifications* – e.g. race, gender, political persuasion, genetics, etc. • *"Sunshine test"* – only use data in ways that would survive if they were out in the "light of day"	• *Set a retention policy for customer data* – tie this to how long this data is useful • *Have a "what data should we keep" process* – periodically determine which data isn't worth keeping. Look at tradeoff between "invasive" and "useful"

ACCION

Design: software security

How do I balance speed and security?

- Focus on the right level of technical security for your stage
- See "Balancing Speed & Security" article →

What types of security testing should I be using? (at a minimum)

- *Automated* – check for common vulnerabilities. Do before you deploy
- *Black box* – tester tries to get into the system from the outside – 3-4x/year
- *White box* – customized; open your system to tester and they try to find vulnerabilities. Look for reputable vendors and perform ~1x/year

What are the most common and dangerous software security risks?

- See OWASP Top 10 article →

Additional resources

- **OWASP Top 10 2017 –** OWASP is an open source group which publishes top security vulnerabilities. Extremely important to review!
- **Balancing speed & security** – article from startup CTO and now security advisor. Great insight into how to think about tradeoffs.
- **Security 101 for startups** – some content relates to software and infrastructure, others more process-oriented
- **Security testing types** – overview of the types of testing available in-market
- **Security fatigue** – balance between security and UX

ACCION

Design: infrastructure security (1/2)

Is it more secure to outsource infrastructure or keep it in house?

- **Generally, outsourcing will be best** – providers such as AWS or Azure will have secure environments which will protect against infrastructure risk
- **Specific situations may change this –** high costs relative to volume used and latency caused by other users may make insourcing better

If I do outsource (e.g. AWS, Azure), how can I ensure I'm protected?

- Cloud infrastructure providers have a range of security services. Here are a few to **ensure you've enabled**:
  - Logging and monitoring with controls (e.g. Amazon Cloudwatch)
  - Identity & access management (e.g. MFA, permissions)
  - Encryption of data at-rest
- See the "AWS Security features" page for additional options →

Additional resources

- Full Infrastructure Checklist – comprehensive list of process and infrastructure checks
- AWS security features and AWS security best practices whitepaper
- Azure security features
- Cisco Checklist – potentially too comprehensive for startups, but useful if using your own data environment
- OWASP Top 10 2017 **–** some OWASP issues touch on infrastructure issues

ACCION

Design: infrastructure security (2/2)

What are some general best-practices for infrastructure security?

General infrastructure	• **Enable cloud infrastructure default security options** • **Back up data at minimum daily, but limit redundancies –** limit number of places that the same data is stored • **Encrypt data while at rest and while in-transit** • **Periodically purge data** – have a retention policy • **Have a BC/DR technology solution and plan** • **Implement patches for known vulnerabilities as soon as possible** – patch managers can help. Definitely by 90 days, preferably within 24 hours.
Passwords & network access	• **Use a password manager** – for 2FA, password recovery, etc. If you don't, ensure security credentials are encrypted • **Password reset** – every 90 days or so • **Tiered access levels** – various access levels to data based on function and level • **Require a secure VPN –** to remotely access network
Scanning & monitoring	• **Implement a simple logging function** – comes with AWS / Azure, or you can purchase for in-house infrastructure • **Include relevant data** – login, logoff, data access, etc. Record (at minimum) username, time, and actions taken • **Create lockout thresholds** – automatically triggered lockout if certain metrics (e.g. no. of logins) exceed threshold

ACCION

Design: partner management

How can I make sure my partners don't open me up to vulnerability?

- **Pre-contract checks** – perform due diligence on new partners prior to onboarding
  - What are their encryption practices (for at-rest and in-transit data)?
  - Have they ever had a breach?
  - What do partners think about their data security practices?
- **Service-level agreements (SLAs)** – common in data-sharing partnerships, SLAs clearly state requirements & reinforce security needs
  - SLAs should be included in data policy, requiring that partners quickly report security breaches
  - SLAs often include the ability to audit & request specific data security standards

How do I ensure my partner management is successful?

- **Learn from partners' suggestions** – more mature business partners will likely have more stringent data security measures than early companies. If they request changes, view this as an opportunity to improve.
- **Continuous monitoring & review** – partner assessments should be performed on a quarterly basis to ensure appropriate levels of access & protection

Additional resources

- Best practices to reduce third-party cybersecurity risk – helpful thoughts on creating a foundation for your company's management of third-party risk
- Approaching data security in a fintech-friendly world – an interesting article that sheds light on how banks may be thinking about partnering with your company (and the associated risks)
- Steps to mitigate 3rd party cybersecurity threats – basic to involved guide to think through partner issues

ACCION

Design: culture

What does a best in class data protection culture look like?

Key beliefs	Practices to reinforce
*"Data security threats are real – **all of us** (not just tech) need to be aware and careful"*	• **Data protection newsletter –** quarterly email to staff. Make this engaging and pithy (have someone in marketing help!) - *Threat data* – summary number of attempts to enter the system, if any were successful, and how the data protection team is following up - *Current events* – share one article and how it relates to the company - *Employee highlight* – public recognition for those who surface issues - *Other content* – phishing quiz, recent examples of risks, repercussions of previous data breaches, process reminders • **Accountable executive for data protection is not just responsible for technology** – perception is critical here - Have *non-technical (i.e. not IT) people train* employees on data protection
*"I want to be **open and transparent** about data protection issues"*	• **Celebrate employees who surface issues** – publicly recognize people who flag security risks or uncover vulnerabilities - During team meetings, "spotlight" developers or employees who have helped - Occasional broader public recognition (e.g. newsletter) • **Don't punish people** who cause security issues – this will lead to people hiding issues rather than surfacing them
*"Data protection is **an ongoing effort**, not a one-time fix"*	• **Blame-free post-mortems** after any security incident to highlight weaknesses in the process which led to issues • **Ongoing "security tracker"** capturing security tradeoffs made in development, then clear the backlog of items every six months
"More sharing = more risk"	• **Limit partner integrations** wherever possible
"Customers don't understand consent"	• **Don't take all customer data, simply because they legally allow us to –** assume some level of consumer privacy protection • **Periodic data "purges"** where we discard data that is not useful for marketing or underwriting

ACCION

Design: data management

What are some best practice processes for data protection?	
Development	• Regular penetration testing (3-6mo black box, 12mo white box) • Security review as part of SDLC
Hiring and firing	• Do reference checks on developers and employees • Ensure digital "locks changed" when employees leave
Reviews	• Hold regular data protection reviews (quarterly)
Miscellaneous	• Do not use USB drives • Encourage auto-lock of laptops (after 5 minutes) • Have automatic locks on your office doors and server rooms • Train employees to not use risky websites on work computer (e.g. pornography, torrents, etc.)

Additional resources

- Security 101 for startups – lots of tangible precautions
- What is social engineering? – highlights the various ways that hackers leverage people rather than technology to gain access

Note: Does not include detail on all processes – some are covered in the culture section

Design: training

What content should I include in my data protection trainings?

	ONBOARDING	ONGOING

All staff	• Our data security culture
	  - **Why** it's important
	  - Key **processes** to prevent + report issues
	  - Key components of the **data policy**
	  - **Role-based** guidelines
	  - Initial **data privacy training**
	• **Types of threats and how we mitigate**
	• Key **data elements**
		• *To be conducted on a regular basis or post-breach*
		• **Regular trainings**: Should cover most common security threats (whether new threats or old), keeping the topic top-of-mind
		• **After a breach:**
		  - Cover **post-mortem** of breach, **updates** to security infrastructure or processes, and any **reporting** line changes
		  - Opportunity for Q&A

Engineering, IT, Data science	*In addition to the above:* • **Legislative & regulatory** environment • **Communication & feedback loops** with non-technical team • Where security sits in the **development process** • **Roles & responsibilities**	• **Monitoring and maintenance** • Updates to data **architecture** and **procedures** • How data security and tech team is **evolving** at pace with company growth, scale, and other changes • **Legislative or regulatory changes**, with implications on data culture

ACCION

Design: breach response (1/3)

What is a data security breach?

- A data breach occurs when a **cybercriminal successfully infiltrates a data source and extracts sensitive information**.
- This can be done physically by accessing a computer or network to steal local files or by bypassing network security remotely.

What should be included in a security breach response plan?

1 Identification & Risk Assessment

- Understand extent of breach
- Assess risks from breach

2 Containment & Resolution

- Form team to lead resolution
- Contain breach, limit damage

3 Evaluation & Improvement

- Review causes of breach
- Understand consequences
- Make process, tech changes

4 Communication

- Plan and execute communication to employees and external parties

Additional resources

- Data breaches 101 – basics details of data security breaches, including examples of major breaches
- Detailed guide for cybersecurity event recovery – from the National Institute for Standards in Technology

ACCION

Design: breach response (2/3)

What are best practices in each phase of a breach response?

	1 Identification & Risk Assessment	2 Containment & Resolution	3 Evaluation & Improvement
Key quesitons	• Understand extent of breach - What **personal data** was involved? - What was the **cause** of the breach? - **How many** people were affected? • Assess risks from breach - What is the **potential for harm** to affected individuals? - What are the **strategic and financial risks**? - What are the **legal or regulatory compliance risks?** - What are the **reputational risks**? - What are the **financial risks**?	• Form team to lead resolution - Who will be **accountable** to contain and resolve? - What **other employees** will be needed? - **How often** will the team meet until resolution? • Contain breach, limit damage - Are we **still vulnerable?** - What **systems changes** are needed to close the breach? - What **process changes** are needed to contain? - How can we **recover damaged or lost data**?	• Review causes of breach – "post-mortem" - What **process or tech vulnerabilities** enabled the breach? - What **other entry points** may have similar vulnerabilities? • Understand consequences - What **consequences occurred to customers** who were impacted by the breach? • Make process, tech changes - What **tech solutions or process changes** are needed? - Should we **modify our data policy**? - What **training** is needed? Other **HR changes**? - What is the **cost** to make these changes? Is it justified?
Best practices	• Initial identification of severity may be incomplete, so **be thorough** as you do forensics • **Do this quickly** – important to understand the situation and respond in a timely manner	• **Key people to include** on team: - Executive accountable for data protection - Legal counsel - Customer service - Technology team • Assign **one person accountability** for each breach • **Not every breach will need everyone** – form team based on severity and cause	• Don't limit evaluation and improvement to purely technical solutions – **spend sufficient time on people and process adjustments** • **Blame-free post-mortems** are key to actually resolving core issues – don't be retaliatory • **Include people from across the organization** (various levels, functions) to ensure buy-in

ACCION

Design: breach response (3/3)

4 ***What communication is appropriate at each stage of breach response?***

	Identification & Risk Assessment	Containment & Resolution	Evaluation & Improvement
	• Understand extent of breach • Assess risks from breach	• Form team to lead resolution • Contain breach, limit damage	• Review causes of breach – "post-mortem" • Understand consequences • Make process, tech changes

Internal	• **Notify groups who interact with external parties**; prepare a "we are working to figure it out" response
	• **Include critical teams** in initial communication
	  - C-Suite, Legal, Technology, PR (if applicable)
	  - Customer service and sales
	  - Board of directors (for more serious breaches)
		• Once cause has been determined, communicate to **employees who could open a similar vulnerability**
		• Provide **regular updates to leadership, legal** until issues are resolved
			• Emphasize that **post-mortem is non-punitive**
			• Include description of what happened and how to prevent in **newsletter**
			• Communicate clearly and concisely about **process and technology changes**

External	• **Be careful about what you communicate externally in the identification and assessment stage** – risk of inaccuracy, inconsistency, or incompleteness
	• Speak to all **relevant external parties**
	  - Individuals affected – often need to do so in <30 days
	  - Data protection regulators
	  - Press / media
	  - Insurers and partners
	• **Always review with legal** before external comms
		• When you communicate, **include all key information**
		  - Description of how and when breach occurred
		  - Data involved
		  - Action taken
		  - Specific and clear advice on what customers can do to protect themselves
		  - How company will support and can be contacted
		• Consider **compensating customers or paying for services** (e.g. ID protection); the **liability of breach consequences should never fall on your customers**
			• Provide **ongoing updates** to customers and partners as you make changes to process and technology

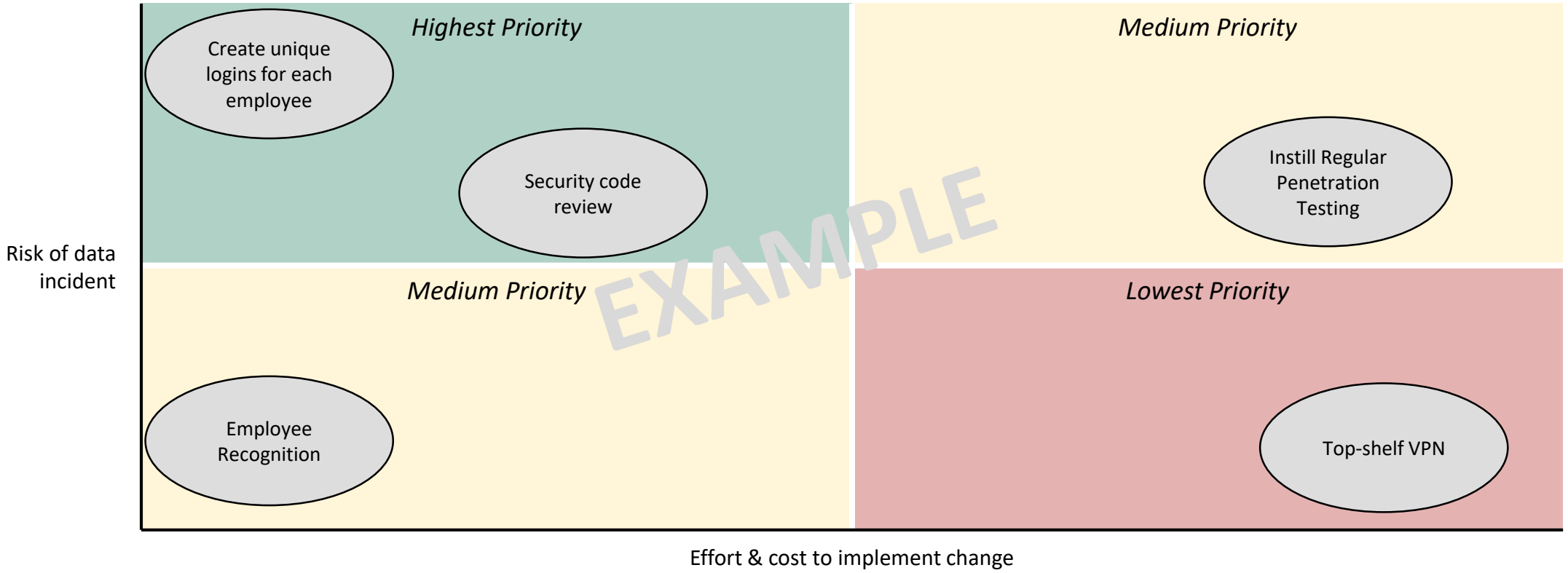
ACCION

Third step to improve data protection: implementation

	Discovery	Design	Implementation
Questions to answer	• What level of data protection is appropriate for our data? • What gaps do we have in our current level of data protection?	• Where do I need to get to on data protection? • What initiatives do I need to put in place to get there?	• How should I roll out changes to data protection in my company? • How can investors test & support pre- and post-investment?
Resources in this guide	• Data audit and risk assessment workshop templates  • Data protection assessment 	• Targeted content on key topics  • Data policy template  • Initiative list template 	• Initiative prioritization template  • Implementation checklist  • Investor diligence & portfolio management guide 
	Click HERE for data protection assessment	Click HERE for data policy template	See appendix of resource for all other blank templates

ACCION

Implementation: Prioritize changes based on risk and effort & cost



Once initiatives are prioritized, implementation can begin

Implementation: checklist from data protection experts

Item	Complete?	Notes
Write down data policy		• Write and review policy with key leaders in the organization and the board
Prioritize data protection initiatives		• Use templates in this guide to identify and select the highest priority initiatives • Focus on the next 12 months – additional for the next 12 month period
Get specific on initiative design		• For high-priority initiatives, define enough detail to be able to implement (e.g. frequency and content of employee recognition) • Include both "hard" and "soft initiatives – technical solutions and process/culture changes • Assign owners and set timelines
Assign accountable executive for data protection		• Single point of contact – ideally with technical and operational oversight
Define metrics and targets		• Use "Metrics" page in this guide for ideas – set targets for priority metrics to track success
Allocate budget for data protection		• Determine funds for personnel, rewards, etc.
Define agenda for data protection reviews		• Use Sample Agenda from this guide, and add other topics as needed
Schedule data protection reviews		• Identify key board, operational, and c-suite team to be part of data protection reviews • Ongoing operational reviews quarterly, annual review

Source: Accion interviews with Cybersecurity experts and CISOs, September 2018

Implementation: sample data protection review agenda

Data Protection Review Agenda*

1. **Follow-up from previous review**
   a. What were the major issues outstanding?
   b. What has / has not been resolved?
   c. What can we do to get closure on these issues?
   d. What are the PR implications? Do we need to react?
2. **New issues since past review**
   a. What new threats or issues have arisen?
   b. What have we done to address them?
   c. What can we do to get closure?
   d. How are we tracking to our metrics targets?
   e. What are the PR implications? Do we need to react?
3. **Recognition and rewards**
   a. Who will be recognized or rewarded based on their contributions to security?
4. **Changes to policy or process**
   a. Do we need to update our data policy based on what we are seeing?
   b. What other process changes might be needed?
5. **Next steps**
   a. Summarize actions from this meeting
   b. Assign timelines and owners

DATA PROTECTION REVIEW BEST PRACTICES

- **Accountable executive should run the meeting** – this includes preparing content (esp. #1, #2 from agenda), calendaring the meeting, sending materials out beforehand etc.
- **Attendees should be positioned to influence process or tech** – likely want to include CISO (if there is one), CTO, COO/Head of Ops, IT analyst who knows the data, and potentially the CEO and HR
- **Focus review on tangible actions** – this is a working meeting where we look to solve problems, not a simple report-out
- **Reviews feed into board report-outs** – in the case of a larger issue, or potentially once per year, board members should be informed of any data protection issues. Data protection reviews can feed into those higher level conversations

ACCION

Implementation: sample metrics for varying stakeholders

Accountable Executive	Cybersecurity / IT Team	Rest of Organization

• Average time required to identify a breach (days)
  - 2017 US benchmark: ~52 days
• Average time required to resolve an identified breach (days)
  - 2017 US benchmark: ~208 days
• Number of remaining unresolved vulnerabilities, by risk level (#)
• Average cost per breach ($)
• Frequency of security review & readouts (days)
	• Percentage of breaches identified in under XX days (%)
	• Percentage of breaches resolved in under XX days (%)
	• Percentage of systems scanned for vulnerabilities, by month (%)
	• Time from identification of vulnerability to creation of patch (days)
	• Number of users with “super user” access level (#)
		• Number of incidents identified (#)
		• Percentage of employees who have completed cybersecurity training (%)
		• Average time from point of breach to customer communication (only if applicable) (days)
		  - Benchmark: ~30 days
		• Average time required to install available software upgrades (days)

Once metrics are agreed, baselines, reporting structures, & readout cadences should be defined between the accountable executive and rest of team

ACCION

Implementation: investor diligence and portfolio management

		POTENTIAL DILIGENCE QUESTIONS	WHAT TO LOOK FOR
Responses are <u>not</u> gating	**Early (Seed/Angel)**	• Who is accountable for data protection today?	• Should have **an individual with clear responsibility**; amount of time dedicated likely minimal
		• What type of data do you collect from your customers? How do you make them aware of this collection?	• Should have **awareness of data collected** & **transparent messaging in place** to inform consumers of the collection • Process **should not seem underhanded or deceptive**
		• How do you ensure that your data is secure?	• Should be cognizant of key risks and **showcase a level of respect** towards their customers; **formal standards may be immature**
		• What data sharing agreements do you have with partners? How are these partnerships managed?	• Should be **aware of all partners**, the **standards** in place to ensure security, and **who has access** to what data
Red flags are gating	**Scaling (Series A)**	*<u>Note</u>: Questions above still applicable – responses should be more mature, with larger emphasis on data security due to scale*	
		• Have you ever had a data breach? How did you handle it?	• Screen for **ability to handle a tough situation** and **ensure response was handled ethically**
		• How often do you run data security tests, either internally or with third parties?	• Company should have a process in place to **proactively identify vulnerabilities**; **formal processes may be immature**
		• Do you have a data policy in place today?	• Do not need one, but should be **aware of what a data policy is** • If one is not in place, should be **addressed early post-investment**

ACCION

Blank templates for use in workshops (see following slides)

	Discovery	Design	Implementation
Questions to answer	• What level of data protection is appropriate for our data? • What gaps do we have in our current level of data protection?	• Where do I need to get to on data protection? • What initiatives do I need to put in place to get there?	• How should I roll out changes to data protection in my company? • How can investors test & support pre- and post-investment?
Resources in this guide	• Data audit and risk assessment workshop templates • Data protection assessment	• Targeted content on key topics • Data policy template • Initiative list template	• Initiative prioritization template • Implementation checklist • Investor diligence & portfolio management guide

Blank templates

[Click HERE for data protection assessment]

[Click HERE for data policy template]

ACCION

Discovery: data protection workshop template (audit and strategy)

What is our data landscape?

Data	Data type	Location	Owner	How used	Who can access

Discovery: data protection workshop template

How essential is data protection for each of our data elements?

DATA ELEMENTS

Discovery: data protection workshop template

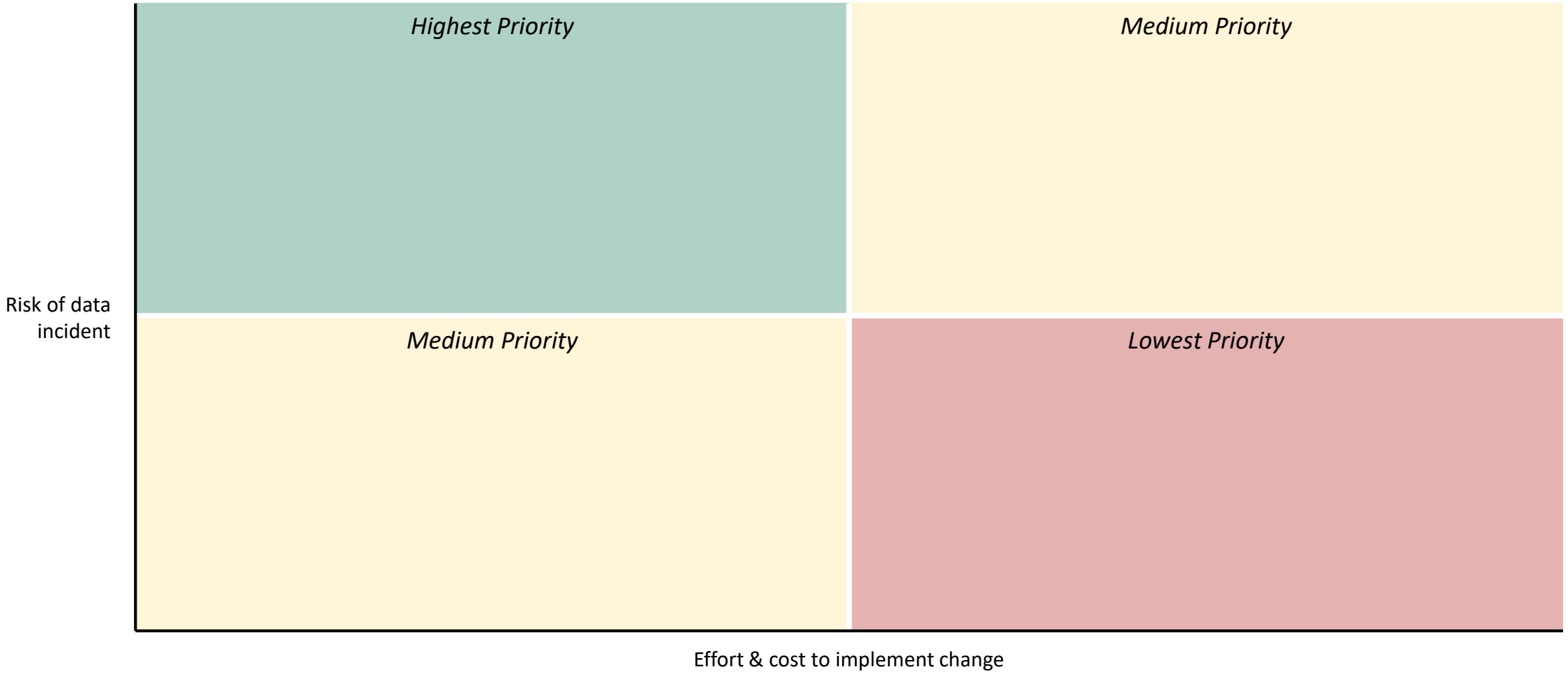
Based on the previous two pages, what risk are we comfortable with on each type of data?

Data	Risk tolerance	Rationale

Design: use policy and vision to create a list of initiatives

Initiative name *How you'll refer to the initiative*	**Policy / Vision** *"Future State" you're working toward*	**How to get there** *Specific changes to process or technology*

Implementation: prioritize changes based on risk and effort & cost



Implementation: checklist from data protection experts

Item	Complete?	Notes
Write down data policy		• Write and review policy with key leaders in the organization and the board
Prioritize data protection initiatives		• Use templates in this guide to identify and select the highest priority initiatives • Focus on the next 12 months – additional for the next 12 month period
Get specific on initiative design		• For high-priority initiatives, define enough detail to be able to implement (e.g. frequency and content of employee recognition) • Include both "hard" and "soft initiatives – technical solutions and process/culture changes • Assign owners and set timelines
Assign accountable executive for data protection		• Single point of contact – ideally with technical and operational oversight
Define metrics and targets		• Use "Metrics" page in this guide for ideas – set targets for priority metrics to track success
Allocate budget for data protection		• Determine funds for personnel, rewards, etc.
Define agenda for data protection reviews		• Use Sample Agenda from this guide, and add other topics as needed
Schedule data protection reviews		• Identify key board, operational, and c-suite team to be part of data protection reviews • Ongoing operational reviews quarterly, annual review

Source: Accion interviews with Cybersecurity experts and CISOs, September 2018