digital defense fund

Organizational Security Basics

Last updated 1/20/21

Developed by Digital Defense Fund, Mari Hernandez, & Quita Tinsley

Development of this presentation

This slide deck was created by Nicole Lopez, Mari Hernandez, and Quita Tinsley for a presentation at the TechForward 2019 conference, “Growing a Culture of Security from the Grassroots”.

This presentation is aimed at non-profit or grassroots organizations leveraging volunteer labor.

Assess your baseline

What is the baseline & how to assess it?

- Takes stock of your org's current security posture
- Asks questions about organizational infrastructure, accounts, policies, etc.
- Informs your areas of focus and priorities
- Attainable from tech and security companies

DIY Baseline Key Indicators

- Does your org use institutional email?
  - Does your org use GSuite, Office365, or something else?
  - Is the personal kept separate from the organizational?
- Account security best practices?
  - Do org members use two-factor authentication?
  - Do org members use password managers?
- Are there any written policies/plans?
  - Confidentiality
  - Onboarding/Offboarding
  - Acceptable Use Policies
  - Data Retention
  - Incident Response and Disaster Planning

ddf

DIY Baseline Key Indicators

- How do people feel about technology and security?
  - Scared?
  - Overwhelmed?
  - Confident?
- How much is tech and security already a part of the convo?
  - Will you be starting these conversations for your org?
  - Are there already security champions in your org?
- Take stock of your existing practices!
  - Do you already delete or redact data? Write it down!
  - Do you auto-rotate passwords? Write it down!
  - Codify your existing practices in policy.

Getting buy-in

Buy-in is *crucial* because the security of the organization depends on individual accounts and actions.

What is compelling for your organization?

- Buy-in for smaller orgs v. buy-in for larger orgs
  - How much face time do you get with staff and board?
- Motivation is different for staff, board and volunteers
  - Board: long-term sustainability and reputation
  - Volunteers: privacy and safety of the community
  - Staff: all these plus responsibility to clients and donors.
- Did you identify any possible tech champions during your baseline review?
  - Already using good practices, background in tech, comfortable talking about it, interested in learning more?

Get your leadership on board

- Tie security to your mission
  - Keeping client data safe is part of the spectrum of services you're providing
- Let the money talk - use data
  - Average fallout of a breach costs $3.92 million (IBM 2019 Data Breach Report)
- Community work is built on trust
  - Will donors continue to donate if they don't trust that their data is secure?
  - Will clients trust you with their information?
  - Will volunteers trust that they are protected? Peer orgs?
- Be persistent

ddf

Exercises to motivate buy-in

- Have folks check haveibeenpwned.com to see if they're on a breach list
- Do a dox yourself exercise - see how quickly you can find the home address, etc of somebody in your org

First one to find someone's address gets a prize!

Threat modeling

Not all people or organizations face the same threats.

What is your context?

What is likely?

INCIDENT TYPE	COUNT OF INCIDENTS	COUNT OF SAMPLE	% OF SAMPLE EXPERIENCE INCIDENT
1. Email Phishing	140	41	26%
2. Malware	54	39	25%
3. Account Compromise	20	18	12%
4. Business Email Compromise	14	13	8%
5. Wire fraud	3	3	2%
6. Virus	1	1	1%
7. Advanced Persistent Threat	1	1	1%
8. Supply Chain	0	0	0%
9. Ransomware	0	0	0%
Grand Total	233	116	50%

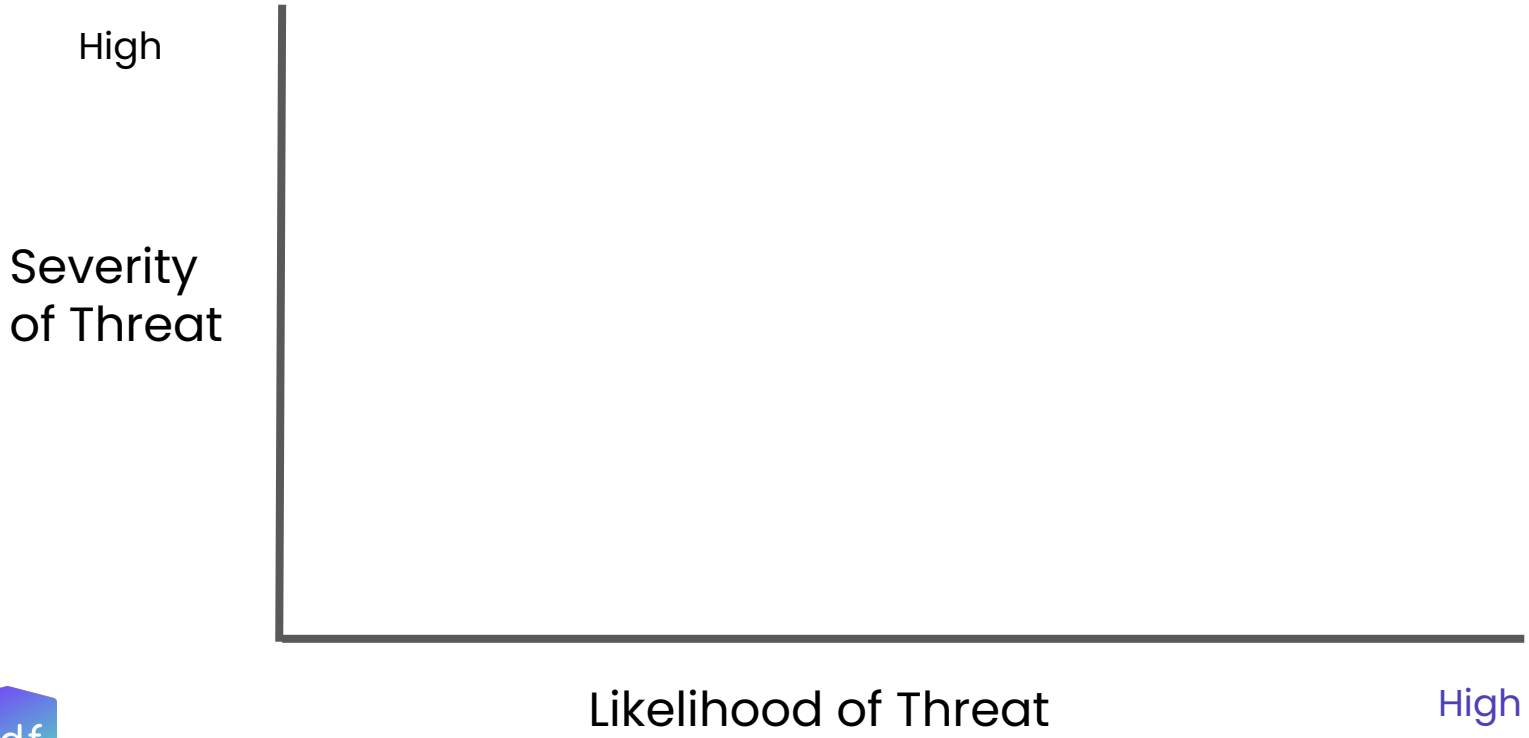
^^ From Community IT's 2018 Non-profit Cybersecurity Incidents Report
https://www.communityit.com/wp-content/uploads/2019/03/NonprofitCybersecurityIncidentReport.pdf

ddf

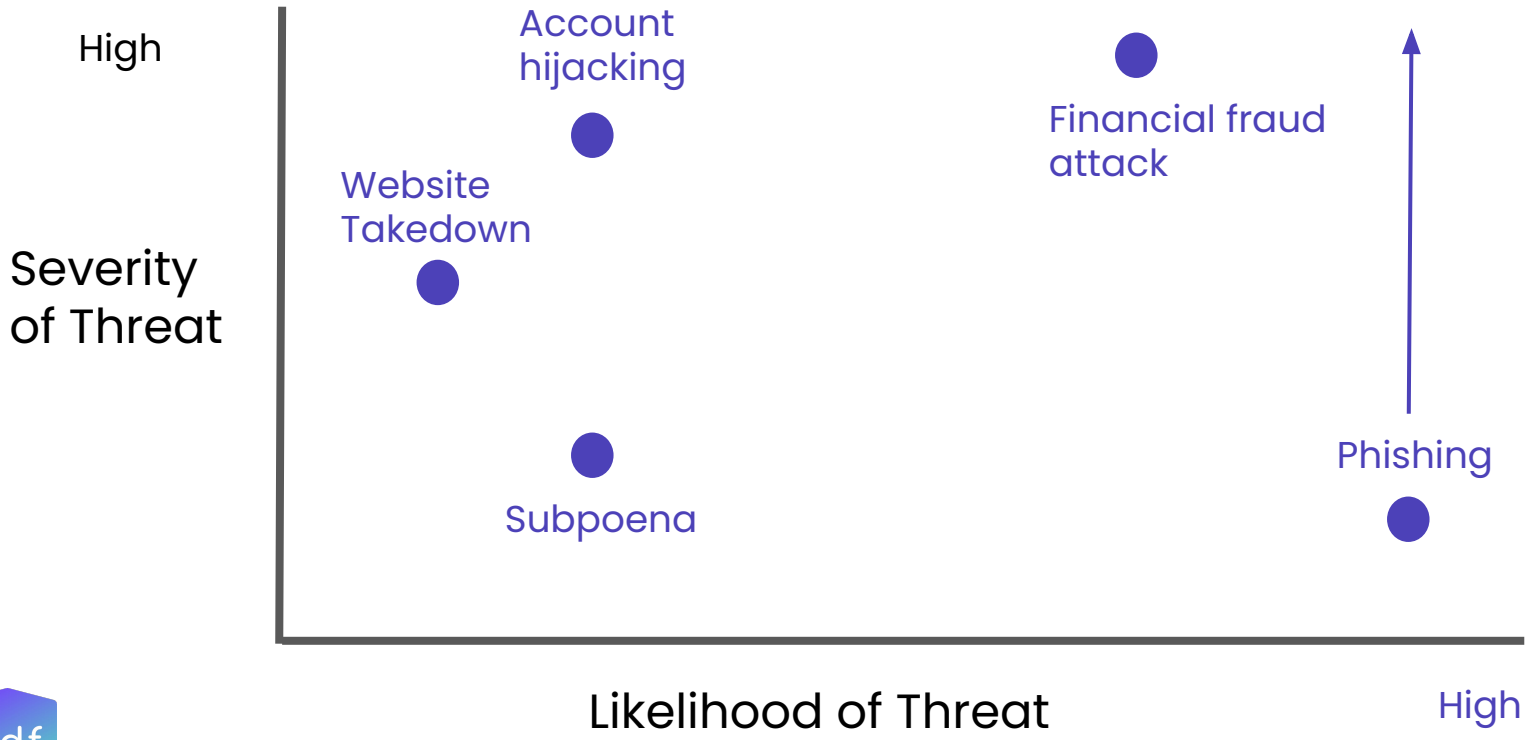
What is likely?

- Lost phone or computer
- Serious illness, injury, or death
- Disgruntled staff, volunteer, organizer

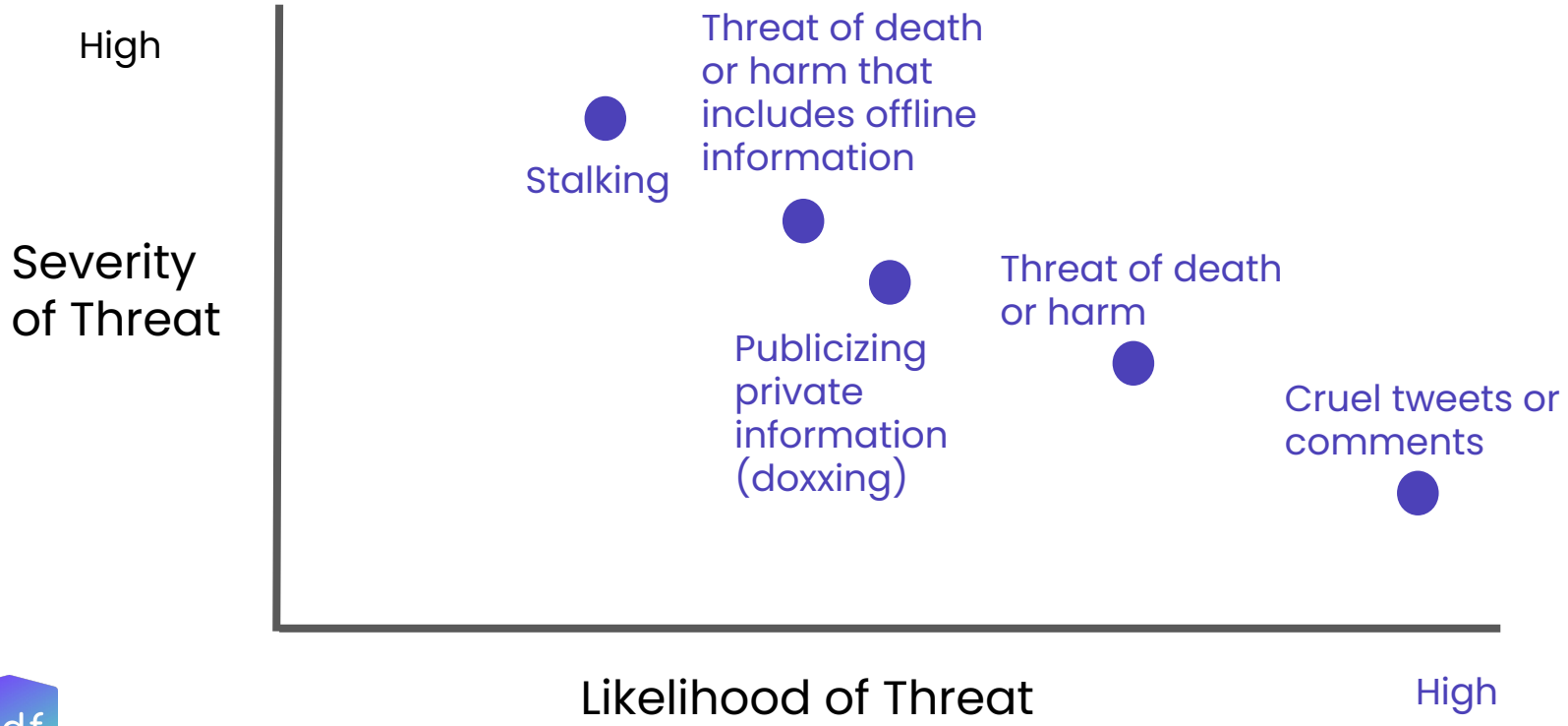
Threat Modeling: likelihood vs. severity



Threat Modeling: non-profit organizations



Threat Modeling: Online Privacy & Doxxing



Threat Modeling: During a Protest

How to build your threat model

What has happened to the org before? What is likely to occur?

Are certain members of the org more visible/public?

Are certain members of the org experiencing harassment or stalking?

Are org members or clients a part of marginalized communities?

Who are the threat actors? Fraudsters? Extremists? Law enforcement?

→ Ground your threats in reality, not fear

ddf

Don’t forget the data!

Questions to ask about the data...

- What data do you collect? Why?
- What data do you share? Why? How? With whom?
- How is your data stored? For how long?
- Would a breach of this data harm people?
  - Immigration data → deportation
  - Abortion data → professional/personal fallout, harassment
- Do we need this data for our operations?
  - Do we need ALL of this data for our operations?
  - Can we make this data anonymous?

Do the benefits of storing this data outweigh the risks?

Where is sensitive data? Who has access?

Map this out with your org

Sticky notes exercise!

- Write down types of information your org holds
- Write down where information lives
- Write down who has access
- Map out high to low impact of account compromise of each of those

→ Prioritize which accounts to secure first

ddf

You know your org
and the threats
you face best!

Start with small steps

Start with key staff and volunteers with more public roles.

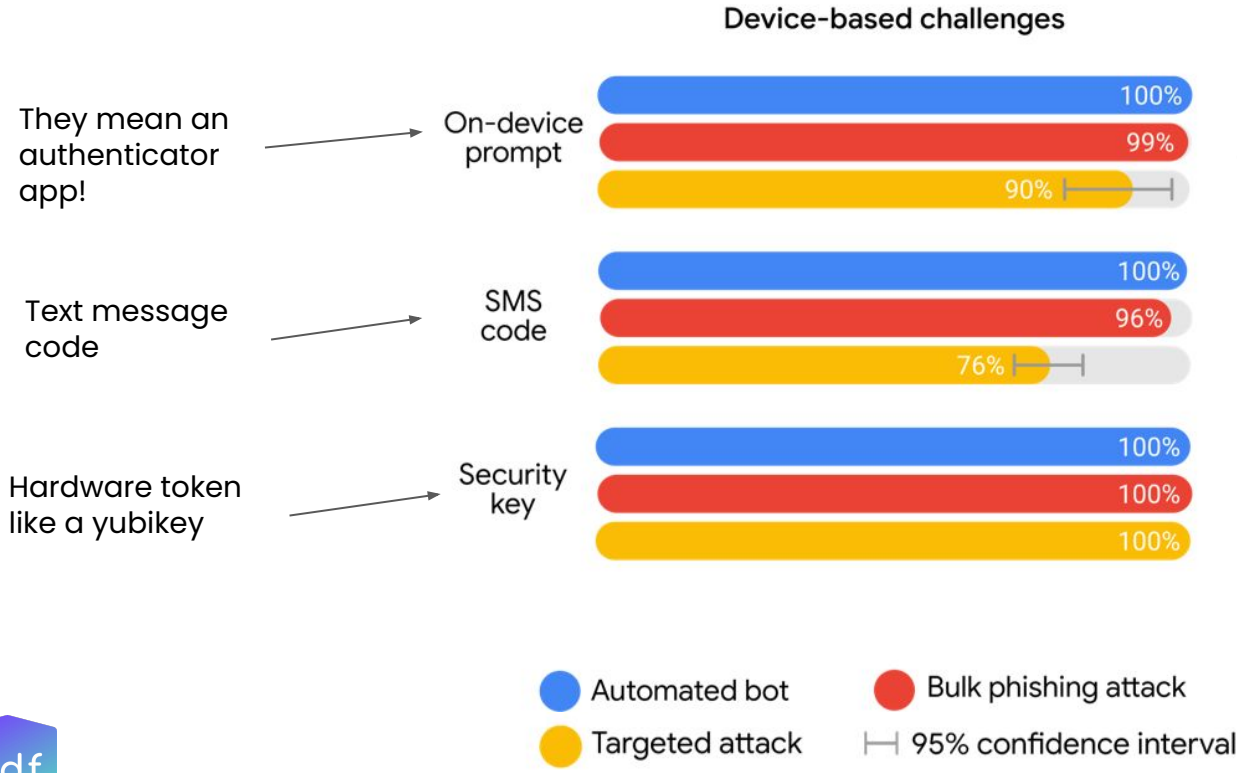
Make it personal, then make it organizational.

Secure social media

- You have to manage Facebook pages and groups through personal pages
- A breach of an admin's personal Facebook page means the organizational pages are compromised
- Facebook being compromised can put your Instagram, email, and supporters at risk

Secure individual accounts by using 2FA and password managers.

2FA: Account Takeover Prevention Rate



100% effective against automated bot attacks

At least 96% effective against bulk phishing

For targeted attacks, SMS and app-based 2FA are weaker

Agree on communication norms

- Agree on how you communicate
- How is sensitive information communicated internally? Externally?
- What belongs in an email vs an encrypted messenger?

Recruit and assemble your security person or team.

Automation & Repetition

- Use a password manager
- Set a calendar reminder to change passwords
- Add security updates to staff and volunteer meetings
- Normalize talking about digital security
- Don’t stress, just keep doing it!

Account Hygiene

ddf

What is account hygiene?

- Not a one size fits all definition
- Refers to best practices for org members and system administrators to use to keep accounts secure

Separate personal from organizational

- If your personal account gets breached, your org is still safe!
- If your org gets subpoenaed, your personal data is protected!
- Easier to know what belongs to the org vs the person

ddf

Staying up-to-date on your app & software updates can prevent up to **85%** of targeted attacks.

Citation: US-CERT

Establish Access Controls

- Does everybody need access to everything?
- Compartmentalize who has access to what
  - Comms folks don't need to be on the bank account
- Write down who has access
  - Establish a backup person
- Make guidelines for sharing access safely

Periodically Review Access

- Take time to revisit who has access
  - Set a calendar reminder
  - Review every time you create a new account or offboard somebody
- Do this for all systems
  - Password manager shares
  - Email accounts
  - Social media accounts

Avoid Shared Accounts

- Shared accounts pool all your risk
- Access is all or nothing
- If one person's credentials are compromised, everybody's access is compromised
- Individual access can't be granted or revoked

ddf

When shared accounts can't be avoided...

- Group email (ex. Google Groups)
- Multiple phone numbers per account (ex. PayPal)
- Shared number (ex. Google Voice) for two-factor authentication
- Share with a password manager
- Rotate your shared credentials

Building security into your existing processes

Support your amazing team

- Implement updates one at a time to not overwhelm individuals
- Utilize regular team meetings
- Have processes ready for when things come up
- Be prepared for questions and feelings
- Listen for feedback
- Create an ongoing conversation

Train your dedicated volunteers

- Remember that all of the volunteers are coming from different starting points depending on experience
  - Do not assume familiarity with or access to devices or apps
- Is there a volunteer coordinator or point person?
- Add security procedures to volunteer handbook
- Make tech security part of the volunteer training day
- Find opportunities to re-train long-term volunteers
  - Tell volunteers about updates - New platform? Mention security!
  - Keep the conversation going!

Educate Your Team About Phishing

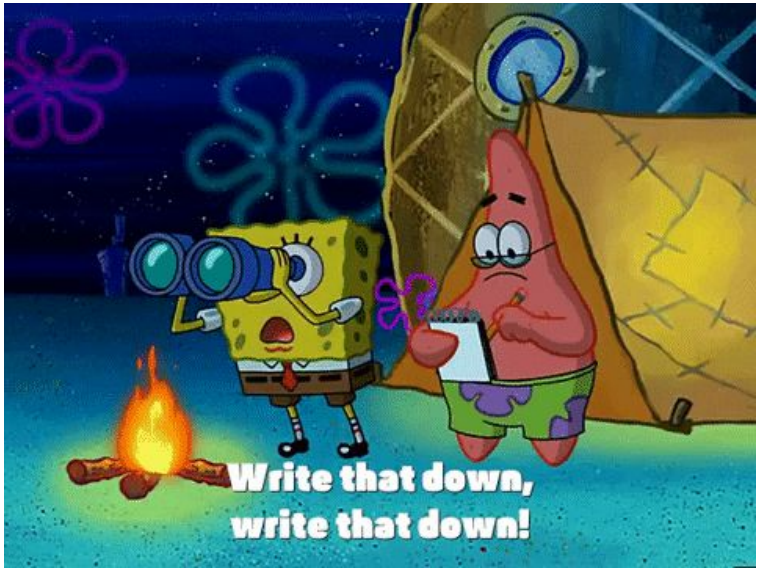
- Check-in with staff when you see suspicious activity
  - Ask staff about login notices
  - Show phishing examples that you come across
- Have a point person or report process for suspicious emails
- Practice. Practice. Practice.
  - https://phishingquiz.withgoogle.com/

Educate Your Team About Phishing

- Check-in with staff when you see suspicious activity
  - Ask staff about login notices
  - Show phishing examples that you come across
- Have a point person or report process for suspicious emails
- Practice. Practice. Practice.
  - https://phishingquiz.withgoogle.com/

Procedures and Operations Handbooks

- Write down processes, even if they are not official
- Is there a procedures or operations handbook for staff?
  - Build on this or make a tech procedures handbook to share
  - Examples: “Don’t post meeting pictures. Use Signal for work text. Password protect your devices.”



Write down what data you store

Type of Data	PII (y/n)	PHI (y/n)	Where is it stored? (use a new line for each integration or service)	How long should we keep it before redacting, archiving, or deleting?	Do retention laws apply to this data?*	How often do we Archive?	How often do we Delete?	How often do we Redact?	What is redacted?
Client intake	Y	Y	Typeform	3 months	Maybe - check with attorney	-	1 year - after annual metrics	3 months	Name, address, email, phone
Client record	Y	Y	Salesforce	3 months after last contact	Maybe - check with attorney	-	1 year - after annual metrics	3 months	Name, address, email, phone
Internal emails	Y	N	Gmail	1 year	N	-	1 year	-	-
Volunteer applications	Y	N	Web form	1 year	N	-	1 year	-	-
Volunteer applications	Y	N	Google Drive	1 year	N	1 year	-	-	-
Volunteer legal docs	Y	N	Google Drive	indefinitely	N	When Volunteer is offboarded	-	-	-
Volunteer background checks	Y	N	Google Drive	2 years	N	-	When Volunteer is offboarded	-	-
Donor records	Y	N	Salesforce	indefinitely	Y - for tax filings	-	-	-	-
Contracts	N	N	Google Drive	5 years	N	5 years	-	-	-
Tax filings	N	N	Google Drive	indefinitely	N	-	-	-	-
Financial reports	N	N	Google Drive	indefinitely	Y - for tax filings	-	-	-	-

ddf

*Sample data retention sheet

Data retention policy should outline...

- What data you collect
- Where it is stored and for how long
- Who is responsible for deleting or redacting data
  - Who takes over if they leave the org or change roles?
- How frequently data is deleted or redacted
- How you will document that this regular deletion or redaction happened

→ Write it down! Revisit every 3-6 months

ddf

Onboarding and Offboarding

- Onboarding - take advantage of new staff training and orientation
  - Have them add 2FA and password app there and then
- Create written procedures
  - Will change depending on role
  - List all technology tools - apps and devices (including work from home)
  - Update as often as necessary
- Have new team member check-ins just about tech security
  - Designate someone to follow up or answer questions
- Offboarding - go through your initial checklists
  - Do not forget to offboard volunteers and board members

Enforcement

- Have an enforcement plan ready from the beginning
- Who will check-in on processes with individuals?
    - Will the enforcer be separate from tech support point person?
- Barriers to compliance: staff is busy, need more information, unsure of timelines

Change your password!

Summary

Cultivating your security culture

- Establish your baseline
- Build trust, get buy-in
- Explain the why with threat modeling
- Break it up into small, digestible chunks
- Practice account hygiene
- Build it into your existing practices