Growing a Culture of Security from the Grassroots

TechForward 2019
Goal of Today’s Session

1. Gain an understanding of the characteristics of grassroots organizations.
Goal of Today’s Workshop

1. Gain an understanding of the characteristics of grassroots organizations.
2. Get some tactical tips for introducing best security practices to your organization.
Goal of Today’s Workshop

1. Gain an understanding of the characteristics of grassroots organizations.
2. Get some tactical tips for introducing best security practices to your organization.
3. Learn from our wins, challenges and pitfalls!
Goal of Today’s Workshop

1. Gain an understanding of the characteristics of grassroots organizations.
2. Get some tactical tips for introducing best security practices to your organization.
3. Learn from our wins, challenges and pitfalls!
4. Get your questions and feedback on how we can together reinforce better practices in our community.
Agenda

● Overview of the grassroots space
● Overview of successful tactics for building a security culture
  ○ Measuring your baseline
  ○ Getting buy-in
  ○ Threat modeling
  ○ Starting with small steps
  ○ Practicing account hygiene
  ○ Building security into existing practices
● Case studies highlighting big wins as well as challenges and pitfalls
● Summary
● Q&A
Where we’re coming from
Abortion Access 101

- Politically contentious work
- Stigma used against clients
- Abortion access groups face unique physical security threats
  - Physical attacks on providers, on-site harassment of clinic staff and clients
- New digital attacks
- Still face general security threats
  - Website security, account security, privacy concerns
  - Client medical privacy
Establishing the Context

Grassroots organizations are often impacted by:

- Not having the resources to hire a security professional
- Everyone is already wearing multiple hats and security feels like additional work
- Decision-making concerns -- who makes the decisions especially in small organizations?
- High turnover
- Reliance on volunteer support
Let's talk tactics
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
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**
Exercises to motivate buy-in

● Have folks check [haveibeenpwned.com](http://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 dox someone gets a prize!
Threat modeling
Not all people or organizations face the same threats.
What is your context?

- Black Lives Matter activists
- Journalists reporting on human rights violations in China
- Environmental activists
- Doctors providing abortions in the United States
- Your organization!
## What is likely?

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

^^ From Community IT’s 2018 Non-profit Cybersecurity Incidents Report
What is likely?

- Lost phone or computer
- Serious illness, injury, or death
- Disgruntled staff, volunteer, organizer
Threat Modeling: likelihood vs. severity

Likelihood of Threat

Severity of Threat

High

High
Threat Modeling: non-profit organizations

<table>
<thead>
<tr>
<th>Likelihood of Threat</th>
<th>Severity of Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>High</td>
</tr>
<tr>
<td>Financial fraud attack</td>
<td>High</td>
</tr>
<tr>
<td>Account hijacking</td>
<td></td>
</tr>
<tr>
<td>Website Takedown</td>
<td></td>
</tr>
<tr>
<td>Subpoena</td>
<td></td>
</tr>
</tbody>
</table>
Threat Modeling: Online Privacy & Doxxing

Severity of Threat

Likelihood of Threat

High Severity

Cruel tweets or comments

 Threat of death or harm that includes offline information

Stalking

Publicizing private information (doxxing)

High Likelihood
## Threat Modeling: During a Protest

<table>
<thead>
<tr>
<th></th>
<th>Severity of Threat</th>
<th>Likelihood of Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photographs taken without consent</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Surveillance by law enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical threats from ID of photos</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ID of photos to target you with online harassment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Arrest by law enforcement</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Photographs taken without consent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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
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
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

They mean an authenticator app!

Text message code

Hardware token like a yubikey

On-device prompt

SMS code

Security key

Device-based challenges

100% effective against automated bot attacks

At least 96% effective against bulk phishing

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

Automated bot

Bulk phishing attack

Targeted attack

95% confidence interval
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
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

Pro tip!
If GSuite or Office365 is out of your budget, make a new free email account
Use a name like:
name.myorg@gmail.com
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
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 co-ordinator 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/](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/](https://phishingquiz.withgoogle.com/)

Pro tip!
Throw a phishing quiz into your regular email or meeting updates!
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

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Data</strong></td>
<td><strong>PII (y/n)</strong></td>
<td><strong>PHI (y/n)</strong></td>
<td>Where is it stored? (use a new line for each integration or service)</td>
<td>How long should we keep it before redacting, archiving, or deleting?</td>
<td>Do retention laws apply to this data?*</td>
<td>How often do we Archive?</td>
<td>How often do we Delete?</td>
<td>How often do we Redact?</td>
<td>What is redacted?</td>
<td>Notes/ applicable laws</td>
</tr>
<tr>
<td><strong>1</strong></td>
<td><strong>2</strong></td>
<td><strong>3</strong></td>
<td><strong>4</strong></td>
<td><strong>5</strong></td>
<td><strong>6</strong></td>
<td><strong>7</strong></td>
<td><strong>8</strong></td>
<td><strong>9</strong></td>
<td><strong>10</strong></td>
<td><strong>11</strong></td>
</tr>
<tr>
<td>Patient record</td>
<td>Y</td>
<td>Y</td>
<td>Typeform</td>
<td>3 months after appointment</td>
<td>Maybe - check with attorney</td>
<td>-</td>
<td>1 year - after annual metrics</td>
<td>3 months</td>
<td>Name, address, email, phone</td>
<td></td>
</tr>
<tr>
<td>Patient record</td>
<td>Y</td>
<td>Y</td>
<td>DARIA</td>
<td>3 months after appointment</td>
<td>Maybe - check with attorney</td>
<td>-</td>
<td>1 year - after annual metrics</td>
<td>3 months</td>
<td>Name, address, email, phone</td>
<td></td>
</tr>
<tr>
<td>Internal emails</td>
<td>Y</td>
<td>N</td>
<td>Gmail</td>
<td>1 year</td>
<td>N</td>
<td>-</td>
<td>1 year</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Volunteer applications</td>
<td>Y</td>
<td>N</td>
<td>Web form</td>
<td>1 year</td>
<td>N</td>
<td>-</td>
<td>1 year</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Volunteer applications</td>
<td>Y</td>
<td>N</td>
<td>Google Drive</td>
<td>1 year</td>
<td>N</td>
<td>1 year</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Volunteer legal docs</td>
<td>Y</td>
<td>N</td>
<td>Google Drive</td>
<td>indefinitely</td>
<td>N</td>
<td>When Volunteer is offboarded</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Volunteer background checks</td>
<td>Y</td>
<td>N</td>
<td>Google Drive</td>
<td>2 years</td>
<td>N</td>
<td>-</td>
<td>When Volunteer is offboarded</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Donor records</td>
<td>Y</td>
<td>N</td>
<td>Salesforce</td>
<td>indefinitely</td>
<td>Y - for tax filings</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Contracts</td>
<td>N</td>
<td>N</td>
<td>Google Drive</td>
<td>5 years</td>
<td>N</td>
<td>5 years</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Tax filings</td>
<td>N</td>
<td>N</td>
<td>Google Drive</td>
<td>indefinitely</td>
<td>N</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>Financial reports</td>
<td>N</td>
<td>N</td>
<td>Google Drive</td>
<td>indefinitely</td>
<td>Y - for tax filings</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>

*note - all documents count under a "litigation hold" or circumstances under which you will be asked to furnish possibly any of these records for pending litigation by opposing counsel.

*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
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!
Case studies
Midwest Access Coalition: transitioning to an encrypted messenger
Midwest Access Coalition: transitioning to an encrypted messenger
Midwest Access Coalition: transitioning to an encrypted messenger

- Added Signal download to volunteer training
- Adding tech and communications standards to policies
- Peer organizations also on Signal
- Everybody loves Signal now!
Midwest Access Coalition: transitioning to an encrypted messenger

- Do your research
- Trust your judgment and expertise
- Don’t start from a place of compromise
- Avoid change fatigue
We’ve Been Attacked...Now What?

Vicious Hack Sends Abortion Fundraisers to Court

“From an account named info@nnaf.org Defendant(s) sent a spoofed email to hundreds of Bowl-a-Thon registrants,” the complaint states. “The email consisted of a picture of a fetus with the message: ‘I hope I grow up big enough to go bowling someday.’”

The NNAF says its expenses related to the hack are still growing.

In addition the the $200,000 bill from a crisis-security firm and attorneys, the NNAF says it had to build a new front-end website, and set up secure hosting and a security audit for the website, at a cost of more than $50,000.

“Over the next couple of hours, the Bowl-A-Thon website appeared to receive $66 billion in fraudulent donations during a distributed denial of service attack (DDoS) which then caused the Bowl-A-Thon website to crash altogether,” the complaint states.
We’ve Been Attacked...Now What?

- We were a new fund and this was our first time participating in BAT.
- Our healthline was not even open yet.
- This cyber attack made us really think about how we needed to protect our callers’ and clinic partner information once we were fully operational.
So how did we move forward?
Moving Forward with a Plan

Slack
- Encryption
- 2FA
- Integrations
- Team Management

Grasshopper
- Virtual
- Custom Number and Extensions
- Team Management

Salesforce
- Encryption
- 2FA
- Password Management
- Integrations
- Team Management
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
Questions?