Data Stewardship + Security Audit

Deeper Dive + Practical Applications

Presenter: Hadassah Damien, security trainer for artists, archivists & LGBTQ community + technologist at the Participatory Budgeting Project. www.femmetech.org

Workshop Goals + Process:

- Interactive online space for you to learn, practice, ask questions
- Review: data stewardship (from Dec) + data security audit (from Nov)
- Look forward to Organizational Planning (Jan)
- Walk through a mini-audit methodology to make it easier to check on your data security as you go.
- Practice and test out some audit questions as a group
- Time for Q&A

PART 1: Review

Data stewardship is a caring approach to data security.

STEWARDSHIP = SECURITY

- Care-full data **collection and storage**: audit (Nov workshop)
- Careful use of **logins**: password managers, 2FA (Nov workshop)
- Careful use of **internet + networks**: Browsing securely, VPN (Dec workshop)
- Careful use of **comms**: Encrypted videos + messaging (Jan workshop!)
PART 2: Clarifying Data Flow

What we can control vs. what we must minimize and plan for

Let’s differentiate **three types of data** that we interact with when we use digital devices:

- Intentional data you’re flowing through your digital devices: sending an email
- Unintentional **METAdata** about your digital devices: an IP address or location
- Protected data that’s within our accounts: the content of a spreadsheet

*Intentional data through your devices*: Is email contents, spreadsheet contents, typing passwords private info. The goal is protecting identity info, and sensitive text (credit card #s, SSNs) in your email or browser from malicious intent, surveillance, or censorship.

*Data about your device*: Is a proxy for you. This is the motherload of trace information that’s collected about each digital user. The goal is to reduce the consumer identity data -- which companies sell, and which can be misused both intentionally and unintentionally. Also addressed here is whereabouts (IP address) masking via VPN, managing phone data, etc.

*Protected data*: Is only as safe as the password managing the account, or the device’s password that might give access to that data, or the physical location of the device. It’s also only as safe as the people using it ensure it to be, considering permissions/sharing etc.

How we control for or minimize risk with these kinds of data:

*Intentional data through your devices:*

- Using HTTPS when we type in browsers to protect content from being read
- Using secure or encrypted video, chat, messaging, email
• Not typing or entering vulnerable info in the first place

Data about your device:

• Using a VPN
• Keeping “location” and GPS off on your phone
• Not being logged in to other platforms using Facebook, shutting down “connected apps”
• Removing extraneous apps from your phone

Protected data in your accounts

• We use passwords for our phones, tablets, and laptops
• We secure those passwords by making them strong and using 2FA where appropriate
• Keep track of digital devices, who’s accessing them, and if they should be accessing them using the accounts they are (loss prevention, onboard/offboarding)

Part 3: Auditing as an Organizational Development Practice

Check in on your data with collaborative Mini-Audits

Mini-audits are great, as they allow you to do low-stakes, ongoing check ins on your team’s approach, and to provide real time support to them and remediation of any issues.

A story: I did a mini-audit of an organization and asked the staff to anonymously tell me how and where they were getting on the internet, and if they had docs on their computers that weren’t on our shared drive. I found that 80% of my staff used cafe and other random wifi networks regularly, and 22% had crucial documents on their computers that
weren’t also on our shared drive. In response I instituted fun security education emails, we put a policy in place for saving documents, and worked with IT to set up a VPN.

The Mini-Audit practice:

- Identify a team, digital asset or platform, or work area to mini-audit based on your risk assessment
- Collaborate to identify issues, grounded in your values and with lots of respect for the practices of your team
- Collaborate on remediation, which may include technical support and policy work, education, and practice.

Examples - Sit with a coworker or team, and together, try asking or exploring:

1) What’s in your email? Have the team do a quick audit of email looking for things you’ve risk-identified. Is there any possibly vulnerable info in there?

2) Tell me how you ________ (fill in the blank based on your risk assessment or something you’ve noticed)

3) Do you duplicate your password?

4) Are you shopping online at work? (looking for viruses coming in)

5) How do you communicate sensitive information to members/clients/staff?

6) How do you share a file? Do you upload it to google drive/ dropbox/ use email attachments?

Part 4: Auditing as a Data Stewardship Practice

Protecting what you’re collecting with mini-audits.
Another story: With my operations team I lead a mini-audit of our shared Drive, first just exploring permissions, and quickly learning we needed to search for “W9s” to see if we could find any out of place (we did). We moved them, changed permissions, updated our larger team, and created a new policy for saving W9s.

**Planning to go forward**: go over what TO do instead with your colleague or team. Practice it once together. Direct support on a password manager, strong passwords, using a VPN, checking for httpS, or installing Signal together could be here.

**Examples** - *Sit with a coworker or team, and together, try asking:*

7) Who do we share google docs with and what’s in them?

8) Can you access it from "outside"? Have you ever tried to open files from outside your network? Checked permissions? Searched for vulnerable data?

9) Look at survey questions, or spreadsheets you've collected data in. You want a snapshot and to share understanding of the state of the security practices, and the tools you have at the moment.

**The Mini-audit practice again:**

- Identify a team, digital asset or platform, or work area to mini-audit based on your risk assessment
- Collaborate to identify issues, grounded in your values and with lots of respect for the practices of your team
- Collaborate on remediation, which may include technical and policy work, education, and practice.

**Taking this back to your organization**

What will help you take this back to your org? Name your next steps and get going!