Data Safety Tools

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Data Safety Tools

As noted elsewhere in this edition of *Risk Management Essentials*, cybersecurity is never just about firewalls and checklists; it requires an organizational commitment to talk openly and transparently about the opportunities and challenges of your team's data-handling practices. However, part of good data hygiene is having tools to do the job. This checklist, reminder list, and emergency reporting protocol are designed to provide another layer of safety for your data by helping your team spot and report potential "silent" data leaks in their daily habits.

The "Human Firewall" Data Safety Checklist

1. **Email & Communication**

- **Check the "To" field twice:** Auto-complete often suggests the wrong person or wrong address. Before hitting send on an email with sensitive info, did I verify the recipient's address?
- **Review for Personally Identifiable Information (PII) in plain text:** Did I avoid putting Social Security numbers, credit card details, or sensitive health information directly in the body of an email?
- **Keep internal matters internal:** Am I using encrypted internal tools (like Slack or Teams) for sensitive chats instead of my personal SMS or WhatsApp?

2. **File Management & Storage**

- **Check the file access status:** When working with cloud folders (Google Drive/SharePoint), do I have the access set to "Restricted" or "Only people in my organization" rather than "Anyone with the link"?
- **Clean up downloads:** Did I delete sensitive reports or donor lists from my computer's "Downloads" folder once I finished uploading them?
- **Avoid using "Shadow IT":** Am I strictly using the organization's approved software, rather than personal accounts or unapproved "free" apps to move data?

3. **Remote & Office Habits**

- **The Multi-Factor Authentication (MFA) Rule:** Is MFA active on every work account I use, especially on my phone?
- **Lock it up:** Do I lock my computer screen (Win+L or Cmd+Ctrl+Q) every single time I step away from my desk, even for a coffee?
- **Physical paper trail:** Are donor checks, printed reports, signup sheets or other hard copy documents stored in a locked drawer rather than sitting on top of my desk?

4. **Device Security**

- **Pay attention to public Wi-Fi use:** Public Wi-Fi is a playground for data sniffers. If I'm working from a cafe, am I using the organization's VPN?

- **Respond to update prompts:** Updates often contain critical security patches for known leaks. Did I click “Install” on that software update today?
- **Follow lost device protocol:** Do I know exactly who to call if my work phone or laptop is lost or stolen?

Red Flag Reminders

If you notice any of the following, report it to IT/Management immediately:

- A “password reset” email you didn’t request.
- A colleague asking for sensitive info via a new or “personal” email address.
- An unexpected pop-up asking you to “re-verify” your login credentials.

Emergency Reporting Protocol: What to Do if You Spot a Leak

If you suspect data has been compromised, lost, or accidentally shared, time is your most important asset. Do not wait to be sure that there is a problem—report what you suspect as soon as possible.

Step 1: The Immediate Notification

- **Primary Contact:** [Insert Name/Title, e.g., IT Manager or Director of Operations]
- **Phone/Extension:** [Insert Number]
- **Email:** [Insert that person’s email or the Dedicated Security Email if your team has one, e.g., security@nonprofit.org]
- **Backup Contact:** [Insert Executive Director or Board Member Name]

Step 2: Contain the Breach

- **Do Not Delete:** If you received a suspicious email or file, do **not** delete it until IT has seen it. They may need it for forensics.
- **Disconnect (If Necessary):** If your computer is behaving strangely (files moving, windows opening), disconnect from the Wi-Fi or unplug the ethernet cable immediately.
- **Change Your Password:** If you think your credentials were stolen, change your password from a **different, secure device** and alert your supervisor so they can reset your account tokens.

Step 3: Document the Details

While the event is fresh, quickly note down:

- **What happened?** (e.g., “I clicked a link,” “I lost my laptop,” “I sent a donor list to the wrong person.”)
- **When did it happen?** (Date and approximate time).
- **What data was involved?** (e.g., Names, credit card digits, addresses, or medical records).

Step 4: Avoid Public Discussion

- **Internal Only:** Do not discuss the potential leak on social media or with external partners until the leadership team has provided an official statement. This protects the organization’s legal standing and donor trust.