

A background network diagram consisting of a complex web of thin, light blue lines connecting various circular nodes of different sizes. The nodes are scattered across the frame, with some larger nodes acting as hubs. The overall aesthetic is clean and technical, suggesting a focus on data, networks, or security.

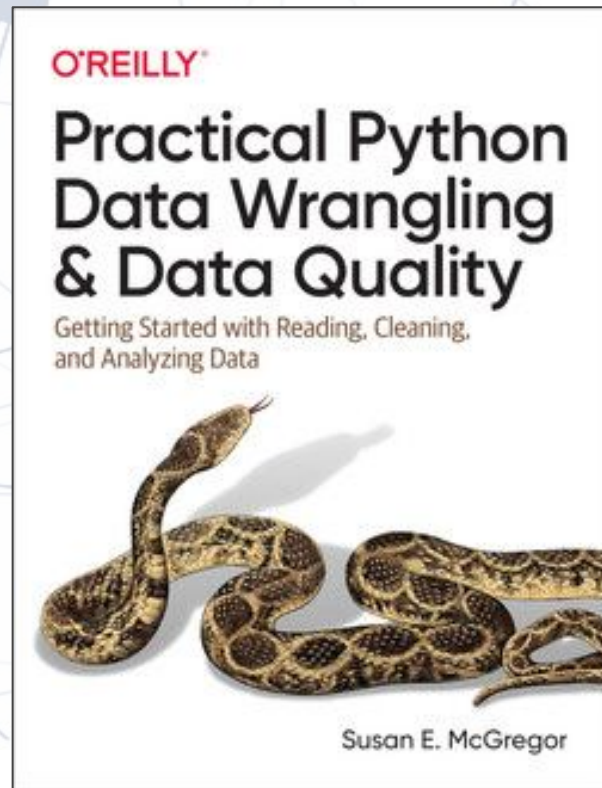
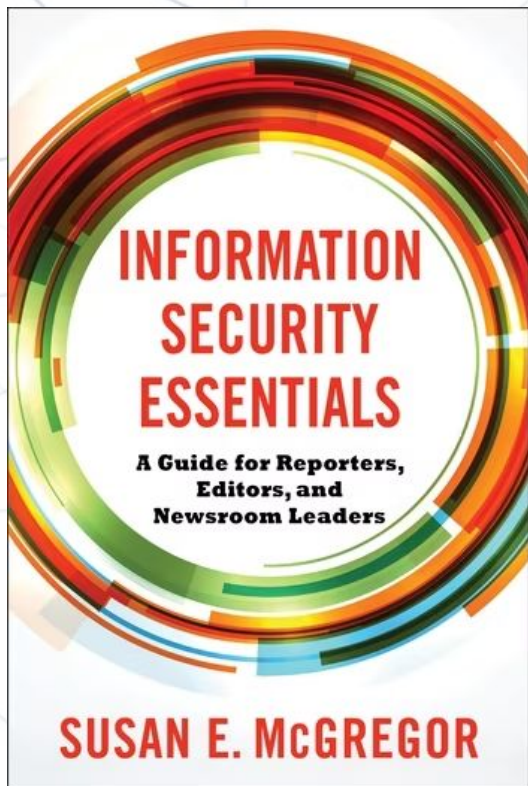
Into the Breach: Strategies for Fully-Scoped Security

Susan E. McGregor

Associate Research Scholar
Co-chair, Center for Data, Media & Society
Data Science Institute
Columbia University

About Me

web development / data science / journalism / security



Information security in development

- Access control/authorization
 - Authentication
 - Encryption
- Data integrity
 - Log forging
 - Data corruption
 - Deletion

Security community: Security is important!

Also security community:

NO SECURITY IS PERFECT



A background network diagram consisting of numerous light blue nodes connected by thin lines, forming a complex web of connections. The nodes vary in size and are distributed across the frame.

Fortunately, when there *is* an (inevitable) security failure, the security community knows just how to help:



or



The background of the image is a complex network diagram. It consists of numerous small, light blue circular nodes scattered across the frame. These nodes are interconnected by a dense web of thin, light blue lines, creating a mesh-like structure. The lines vary in thickness and orientation, some forming straight paths while others curve. The overall effect is that of a digital or social network. In the center of this network, the text "WE CAN DO BETTER" is displayed in a bold, dark blue, sans-serif font. The text is horizontally centered and stands out clearly against the lighter background.

WE CAN DO BETTER

What is "fully-scoped" security?

1. Acknowledging that security is about both prevention *and* recovery
2. Recognizing that even if a security failure is not our fault, it's still our problem
3. (Mostly) engaging, rather than blaming, stakeholders

A network diagram consisting of numerous nodes (represented by circles of varying sizes) connected by thin, light blue lines. The nodes are scattered across the frame, with some larger nodes acting as hubs. The overall structure is a complex, interconnected web.

BUT HOW?

Existing security measures: prevention

1. Access control
 - Authentication
 - Roles
2. Encryption
3. Static analysis
4. Secrets management
5. Tech-specific best practices

Fully-scoped security: prevention

Add:

1. Data minimization
2. De-identification
3. Differentially private/synthetic data
4. Offline/cold storage

Fully-scoped security: recovery

Plan ahead for:

1. Notification
2. Assistance/remediation
3. Redress

Most importantly: evaluate and test these approaches *in advance!*

A background network diagram consisting of numerous light blue nodes of varying sizes connected by thin, light blue lines. The nodes are scattered across the frame, with some larger nodes acting as hubs. The overall appearance is that of a complex, interconnected web or graph.

THE EQUIFAX BREACH: A COUNTER-EXAMPLE CASE STUDY

Notification



Equifax's own official channels referred customers to a fake (fortunately white-hat) website. Ensuring that your notification channels can handle the traffic if a major breach happens is essential.

Assistance/remediation



Product Reviews Deals News Action Mission



Sign In

Become a Member

Donate

Electronics & Computers / Is Equifax's Free ID Protection Service Good Enough?

Is Equifax's Free ID Protection Service Good Enough?

How to know if selecting this security option is the best move for you

By Jeff Blyskal

October 4, 2017

Equifax is offering the 145.5 million people affected by its security breach—as well as anyone else—a free, one-year subscription to TrustedID Premier...be aware that **most of them aren't very secure themselves**. Access to your identity protection account is commonly protected by a username and password, which can easily be hacked.

“We recommend a credit freeze instead of identity protection because it’s cheaper and better,” says Anna Laitin, director of financial policy at Consumers Union.

Equifax's assistance and remediation options were themselves lacking basic security measures. Thinking through the impact of a breach on customers and identifying what they might need (even - and especially - if it's not another one of **your** products) is key.

Redress

equifaxbreachsettlement.com



During the Extended Claims Period, impacted class members may submit claim(s) for cash reimbursement. You may be eligible for the following reimbursement cash payments for:

- **Time Spent** during the Extended Claims Period recovering from fraud, identity theft, or other misuse of your personal information caused by the data breach up to 20 total hours at \$25 per hour.
- **Out-of-Pocket Losses** during the Extended Claims Period resulting from the data breach up to \$20,000.

In order to submit a claim for Time Spent or Out-of-Pocket Losses during the Extended Claims Period, you must certify that you have not received reimbursement for the claimed loss through other means.



Free Identity Restoration Services: You will be eligible for at least 7 years of free assisted identity restoration services to help you remedy the effects of identity theft and fraud. Services will be available for at least 7 years after January 11, 2022 (the Settlement Effective Date).

Different harms require different forms of redress. In some cases, expert assistance might be more important than financial remuneration - but whatever the approach, consider carefully what you require for customers to receive it. Onerous processes may reduce upfront costs, but will do little to restore your reputation with customers, which is often invaluable.

A network diagram with nodes and connecting lines. The nodes are represented by circles of varying sizes and shades of blue and grey, connected by thin, light blue lines. The background is white.

HAS ANYONE DONE THIS RIGHT?

"Over"communication and meaningful action

The Tylenol murders

- In the early 1980s, someone laced Chicago-area Tylenol capsules with cyanide, which killed several people. The company issued a massive recall, offered product exchange and a bounty. They changed both the pill and the packaging to be tamper-resistant.

FireEye and SolarWinds

- The companies made frequent updates and disclosures regarding known vulnerabilities and took ownership for the fallout. They also developed and shared countermeasures that went beyond the direct impact of the breach.

Fully-scoped security for developers: what you can do

1. Ask questions! Even (especially) if you think your clients do not know the answer. For example:
 - "How do you want to be able to access this data?"
 - "How often do you want to make an offline backup?"
 - "How often should this be overwritten?"
 - "How do you want to handle data deletion requests?"
2. Make checklists
 - How often to update software/certificates
 - How to audit access, downloads, etc.

Into the Breach: Strategies for Fully-Scoped Security

Special thanks: [Jess Grider](#), [Angel Venchev](#)

Susan E. McGregor

Associate Research Scholar
Co-chair, Center for Data, Media & Society
Data Science Institute
Columbia University