RSA Conference

Where the world talks security

Top Privacy Issues for Infosec Professionals

Gregory Reid, CEO, InFuture LLC

Sam Pfeifle, Content Director, International Association of Privacy Professionals (IAPP)

RSA Conference

Where Security Meets Privacy

Why privacy may very well be an infosecurity professional's best way to move up in the world

Privacy makes data security a regulatory issue

- Federal Trade Commission
  - The FTC has made “reasonable data security” a legal obligation. The FTC’s documented approach includes:
    1. **Take Stock** (You need to know what PI you have stored and where it is located)
    2. **Scale Down** (Minimize it)
    3. **Lock It** (Self-explanatory: Physical, Electronic, Processes, Education)
    4. **Pitch It** (A good case for solid Records Management implementation)
    5. **Plan Ahead** (for the Eventual Breach)

  - Watch the LabMD case – even with no demonstrable “harm,” the FTC took action

Privacy makes security a regulatory issue

- EU General Data Protection Regulation (GDPR). Some examples:
  - Data protection must be built into the system “By Design and by Default”. (Recital 78 and Article 25)
  - Data must be secured using technical means. (Recital 49 and Articles 5-1(f), 32-1(b-d))
  - A determination must be made *almost immediately* as to whether a data breach is likely to have a “high risk to the rights and freedoms of the natural person”, as such a technical environment must be in place to identify, track and assess such breaches. (Recitals 85, 87 and numerous Articles)
  - Infringement fines can range up to €20,000,000 or 4% of the *global* revenue of the organization, which ever is higher, PER incident.

Privacy makes security a regulatory issue

- The greatest challenge in Privacy and establishing a security environment to legally support it are the greatly divergent laws and regulations:
  - Industry: E.g. HIPAA and HITECH (Healthcare)
  - US State: E.g. Massachusetts (201 CMR 17.00)
  - US Regulatory Body: E.g. Federal Trade Commission
  - Other Countries and Bodies: E.g. EU Directive and GDPR, Canadian PIPEDA, Chinese CPL

  Which can individually impact:
  - What the definition of 'personal data' is. And there can be more than one type of data...
  - How personal data is secured, stored, located, managed, accessed, controlled, and processed physically and electronically.
  - And … the legally required breach preparations and breach responses.
- **The key is understanding what the company is accountable for following.**

Privacy makes security a regulatory issue

- The “Good News” is that many of the security obligations are similar across the privacy laws and regulations:
  - Encrypting personal data is almost a universal requirement, on any device or DB
  - Anonymizing or Pseudonymizing data, where possible, is highly recommended
  - Data minimization and deletion traverses many different laws and regulations
  - Keeping an accurate inventory of personal data state, location, and owner is key
  - The technical environment must be secured using "reasonable”, “state of the art” technologies and procedures. (e.g. two factor authentication for admins)
  - Breach preparation, notification, and response processes must be documented, trained and tested. Appropriate resources need to be available

Privacy makes security a regulatory issue

- So, be able to document what you're doing and why
  - You should have a plan and follow it accordingly
  - Monitor "best practices"
  - Record decisions and why you made them
  - Have documentation of the overall plan in a format that the privacy department can explain to the regulator

Privacy makes security a regulatory issue

- Do everything right, and you're vitally important
  - Move from operational to strategic
  - Help privacy show accountability
  - Get a seat at the privacy table – collaborate with the general counsel, CIO, other high-level strategic operators

RSA Conference

“Personal” and “sensitive” data

Sometimes it’s not always obvious which data needs the most protection and proper handling

Definition of “personal” data

- Anything that establishes a 1-to-1 relationship
  - “Telephone book” data may not be particularly “personal”
  - Unique identifiers: IP addresses, usernames, etc.
  - Watch out for combinations of “innocuous” data that, together, can identify a single individual.

Definition of “sensitive” data

- How could the data be used?
  - Health data (fullz)
  - Protected classes
  - Pay attention to jurisdiction

PI is Insidious! (Def'n: *Treacherous, Crafty, Gradual, Subtle*)

- PI and Sensitive PI exists about everywhere … It just creeps:
  - Typical RDBMS transactional environments (ERP, HR, G/L, etc.)
  - User Laptops (in all types of locations. Such as email clients, HD folders, Evernote, screenshots, etc.)
  - User Mobile Devices (and the BYOD ones, as well)
  - Shared Drive/Folder Servers
  - External Shared Drives (Box, Dropbox, Googledocs, etc.)
  - Email Systems (Exchange, Gmail, Yahoo)
  - Content systems (SharePoint, Office 365, Livelink, Documentum)
  - Paper notebooks
  - PLUS all of your third-party information partners and outsourcers (e.g. HIPAA business associates and GDPR processors)

- Privacy laws still cover all these physical and electronic locations, with very few exceptions
- All of these locations need to be, by law, technically, procedurally, and administratively secured

RSA Conference

Where Security and Privacy collide

Sometimes good security means collecting or sharing personal information.

Watch what you collect

- Data minimization
  - You can’t lose what you don’t have
  - Multiple jurisdictions – U.S., EU, and more – emphasize this point
  - Must have documentation – find it and then delete it

- Watch your vendors, too
  - If you’re sharing data, you’re responsible if they lose it or abuse it
  - Are you auditing them on a regular basis?

Watch what you collect

- Log files and authentication
  - When you create an account, you create PII
  - Data retention: How long do you need to keep that log file?
- Physical security issues
  - Single credentials and employee monitoring
  - Theft prevention and customer monitoring

Watch what you share

- CISA and information sharing
  - Can you redact?
  - How much information is helpful? How much is overkill?

- Working with law enforcement
  - What's your company's stance on law enforcement requests?
  - Can you ask them to narrow their focus?
  - Watch out for cross border transfer

You might not care, but does privacy?

- What do the access logs tell you?
  - Peeking, snooping, etc.
  - Are security and privacy policies in alignment?
  - EU laws are quite strict around tracking and storing device data that we take for granted in the US. And the fines are very high. But there are ‘derogations’ for using user data to ensure that your system is secure, if it is solely for that purpose and stored no longer than necessary.

- You can’t take it with you…
  - Intellectual property can be PII, too

RSA Conference

Privacy (and security) by Design

The SDLC, preparing for the worst, and more

The SDLC, Data Security and Privacy Intersection

- You design for security, take one step further for privacy by working with the Developers on their efforts:
  - The Software Development Lifecycle (SDLC) directly supports your abilities to make your technical environment secure.
  - The developers' data architecture designs and data transport layer designs

Preparing for a breach

- There are many, many great articles and plans available on the internet for breach preparation. For example, Experian has an excellent Data Breach Response Guide.

- A couple of short thoughts:
  - Different privacy laws require different breach responses and timeframes which, in turn, require different breach planning processes to support the responses. (HIPAA v. GDPR)
  - Data minimization means **way** less risk down the road. *Electronic Records Management, one more time… And that includes email.*
  - Forensics efforts might introduce privacy risk in themselves (cross-border data transfer?)

Summary Points

- The InfoSec role is critical to privacy efforts. Without it, privacy operations would be impossible to conduct.
- Coordination and clarity between the CIO/CISO, the GC, and the Compliance group is required to meet privacy obligations. No Person is an Island.
- No laws note the requirement for “Superhuman” or “Extraordinary” security efforts. The words “practicable”, ”reasonable”, “industry-standard” are commonly used. However, “Proactive” and “By Design”, not “Reactive” are common themes.
- Many of the laws and regulations have similar, if not the same, technical, procedural and administrative security requirements. Leverage them.
- PI can be in any number of different repositories. You’re responsible for securing all of them; not just the obvious ones inside of RDBMS’.
- TBD