

# Applied Privacy and Security

... practical  
strategies you can  
use!

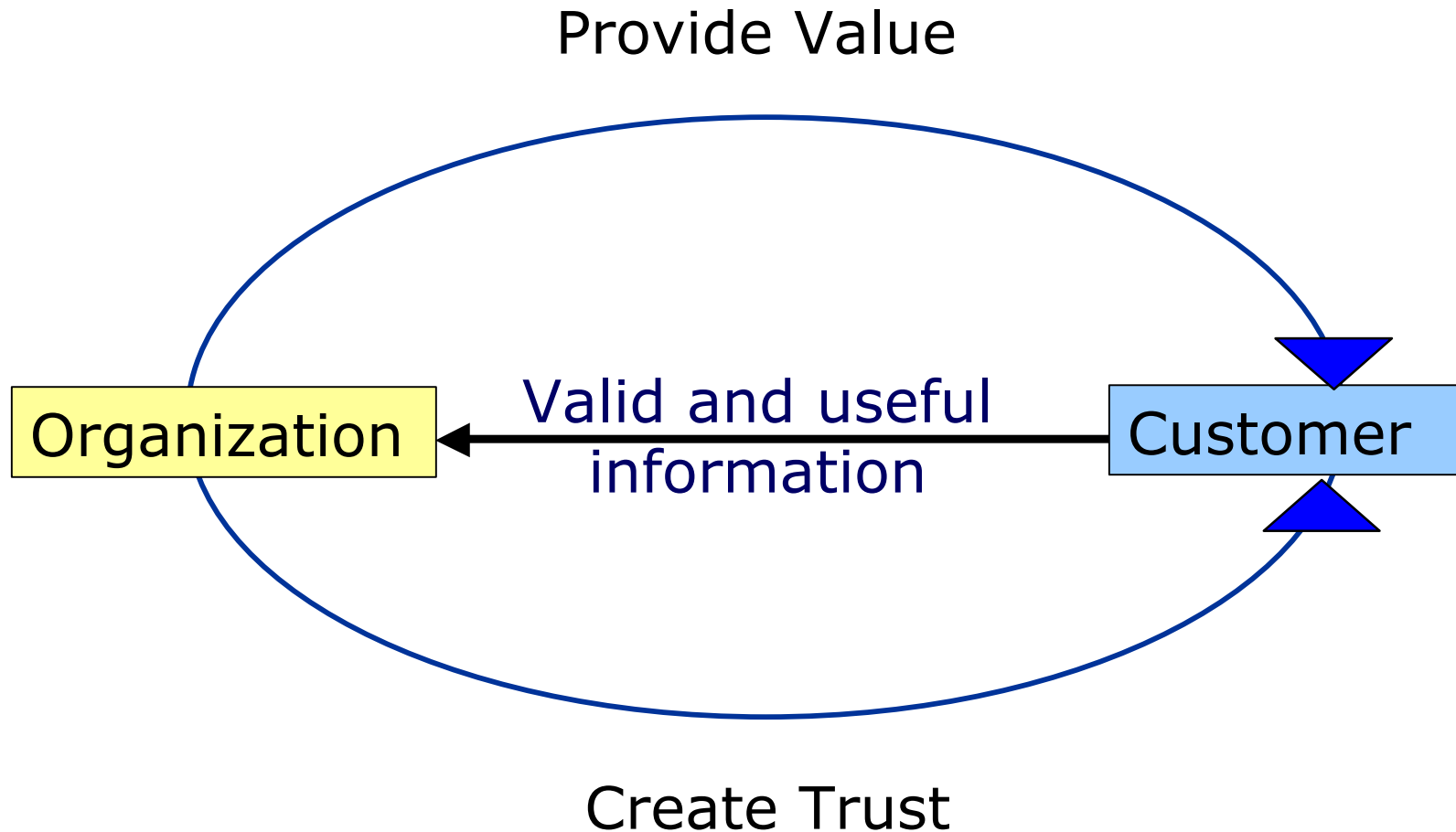


**APSGroup**

Your privacy and security management partner

# The Privacy Exchange

---



# Privacy Violators – How to Punish?

---

Percent who think privacy violators should be punished 94%

## Suitable punishments:

Public blacklisting of site 30%

Site should be shut down 26%


Company should pay fine 27%

Owners should go to prison 11%

Source: Aug. 2000 survey 'Trust and Privacy Online', conducted by the Pew Internet and American Life Project


# Fair Information Practices

---

- 
1. Accountability
  2. Identifying Purposes
  3. Consent
  4. Limiting Collection
  5. Limiting Use, Disclosure, and Retention
  6. Accuracy
  7. Safeguards
  8. Openness
  9. Individual Access
  10. Challenging Compliance

# FIPs- What's the Highest Risk?

---

- 
1. Accountability
  2. Identifying Purposes
  3. Consent
  4. Limiting Collection
  5. Limiting Use, Disclosure, and Retention
  6. Accuracy
  - 7. Safeguards**
  8. Openness
  9. Individual Access
  10. Challenging Compliance

# The Paradigm

---

**It's not about  
Privacy *versus* Security**

**It's that  
Privacy *NEEDS* Security!**

# Food For Thought

---

“When entrusted to process,  
you are obligated to safeguard.”

Bob Johnson, CISSP

former Director of Communications, (ISC)<sup>2</sup>

# Provocation

---

“Hey, we can deal with this privacy and security stuff later. Right now we have too many important things to do, like adding functionality and hitting our deadlines...”

Anonymous



# Start at the Beginning

---

- Deal with privacy and security issues at the beginning rather than forcing it in at the end!
  - Business case
  - Project planning & feasibility studies
  - Development and testing
  - Change management

# Supporting Players

---

- Other corporate policies should support or reference privacy and security efforts
  - Provide guidance to employees, business partners, contractors, etc.
  - Set expectations and avoid confusion
  - Provide guidance on who to contact and how to raise privacy / security related concerns

# Supporting Players

---

- Security policy
- Acceptable use policies
  - E-Mail
  - Internet
  - PCs, laptops, PDAs
  - Cell phones, telephones, modems, faxes
  - Other Corporate Resources

# Supporting Players

---

- Appropriate use policies to support privacy
  - E-Mail
  - Internet
  - PCs, laptops, PDAs
  - Cell phones, telephones, modems, faxes

# Supporting Players

---

- Conduct regular privacy audits
- Make privacy impact assessments part of business cases and feasibility studies
- Conduct regular security audits

# Provocation

---

“As long as I put some policies in place and set some rules to protect the information I keep, I’ve got this privacy thing covered...”

# Information Management

---

- Corporate records management
- Data inventory and classification
  - What information is collected and available
  - How & where information is collected
  - Why is it collected
  - Who sees it and when
  - How sensitive is it
  - Consent requirements (to collect or release)
  - Retention and destruction

# Information Management

---

- Potential benefits
  - Helps decide level of protection needed for data combinations
  - Streamline collection processes
    - Which sources are most current
    - Which sources are most accurate
    - Avoid duplication of efforts
  - Eliminate unnecessary data
    - Reduce storage requirements & costs
    - Can't lose what you don't have!



# Provocation

---

“We just follow the instructions that come with the software... the vendor’s defaults are good enough for us...”

Anonymous

# Protection by Default

---

- Protect everything as a default
  - Don't rely on vendor default settings
  - Only allow access by authorized users for authorized business purposes
  - Easier to grant access than try to figure out if information has inadvertently been left "in the open"
  - Propagate same levels of security if file is moved or copied
- Don't forget to protect any back-up and log files as well!

# Provocation

---

“So, everything is now protected by default, and only a few of us are using the systems, we all trust each other, so what is this authorized users stuff?”

Anonymous

# Everyone's Unique

---

- An important precept is accountability
- Each person accessing information in your charge should have a unique user identification (user-id)
  - Easier to assign individual access privileges
  - Easier to assign temporary access privileges
  - Easier to rescind individual privileges
  - Track access to address accountability

# Origins

---

- Limit access based on location
  - inside your trusted network
  - outside your trusted network
    - dial-up, dedicated line, or VPN
    - wireless
    - over the Internet
- Limit access by date and time

# Provocation

---

“Passwords are such a nuisance, but I make my life simple by having just one that I use for everything, and I don't have to write it down because it's easy to remember – it's my husband's name...”

Anonymous

# Beyond Passwords

---

- Access to your information systems should at *minimum* require a unique user identifier & password in combination
- Remote access should consider using additional multi-factor authentication
- Extremely sensitive information might also require additional authentication
- Consider encryption when storing or transmitting extremely sensitive information.

# Beyond Passwords

---

- Don't allow "remembering" of passwords by programs at log-in
- Don't hardcode passwords in scripts
- Files on laptops should be encrypted
  - Better still, do not allow sensitive files on laptops, etc.



# Provocation

---

“OK, I’ve limited who can get at the personal information we do keep. That’s all I should need to do — it’s not like I have to know every time anyone has seen someone’s personal information.”

Anonymous

# Keeping Track

---

- Knowing what has happened to data or information is integral to privacy and security efforts
- Privacy & disclosure breaches are rarely committed by changing information, usually only access is involved
- Most systems only track changes to data; many don't even track changes!

# Keeping Track

---

- Comprehensive logging capabilities
  - read only or browse access
  - update / modify
  - create / delete
  - failed access attempts
- Log records should show at minimum
  - date and time of access
  - user-id
  - some details of record being accessed
  - access type

# Provocation

---

“After I delete the files and format the drive, no one will be able to get at the information...”

Anonymous

# Gone but Not Forgotten

---

- Deleting file does not mean information it contained is no longer available
- Recovery tools readily available
- Possible courses of action
  - Encrypt file several times before “deleting”
  - Use a good quality “shredder” program
  - Physically shred or destroy media

# Gone but Not Forgotten

---

- And don't forget about other data...
  - back-up copies
  - PCs being replaced, sold or re-cycled
  - PDAs, laptops, cell-phones, etc.
  - hard drives being replaced
  - floppy diskettes
  - CDs and DVDs
  - voice mail systems
  - access cards and badges

# Provocation

---

“So I’ve got policies, and accountability, and I keep logs, and I destroy old data, etc. That’s it. I’m done!”

Anonymous

# Paper Trails

---

- Printed reports need to be handled with the same diligence as computer files.
- Keep track of where reports with sensitive or confidential data are distributed
  - Review reports to see if really needed
  - Limit distribution of sensitive reports
  - Provide lockable cabinets for report storage



# Paper Trails

---

- Disposing of reports with sensitive or confidential data
  - Provide heavy duty shredders so staff can dispose of reports when done
  - Shred material before re-cycling
  - Don't use drafts as scrap paper

# Provocation

---

“Okay, now I get it. I’ve got everything covered. No hacker is going to break into my system and steal my customer data.”

Anonymous

# Threats From Within

---

“The greatest security asset, and the greatest security risk”

- Background Checks
- Confidentiality and Disclosure
- Monitoring and Surveillance
- Subcontractors

# Provocation

---

“We got rid of most of that problem, because we’ve outsourced this area!”

Anonymous

# Get it in Writing

---

- Make sure business partners align with your privacy and security efforts
- Adherence to your organization's IT privacy and security policy / practices should be included in:
  - confidentiality agreements
  - contracts and service agreements
  - non-disclosure agreements
  - outsourcing agreement
  - termination agreements
- Ensure you have the right to audit their practices

# Quotable Quotes...

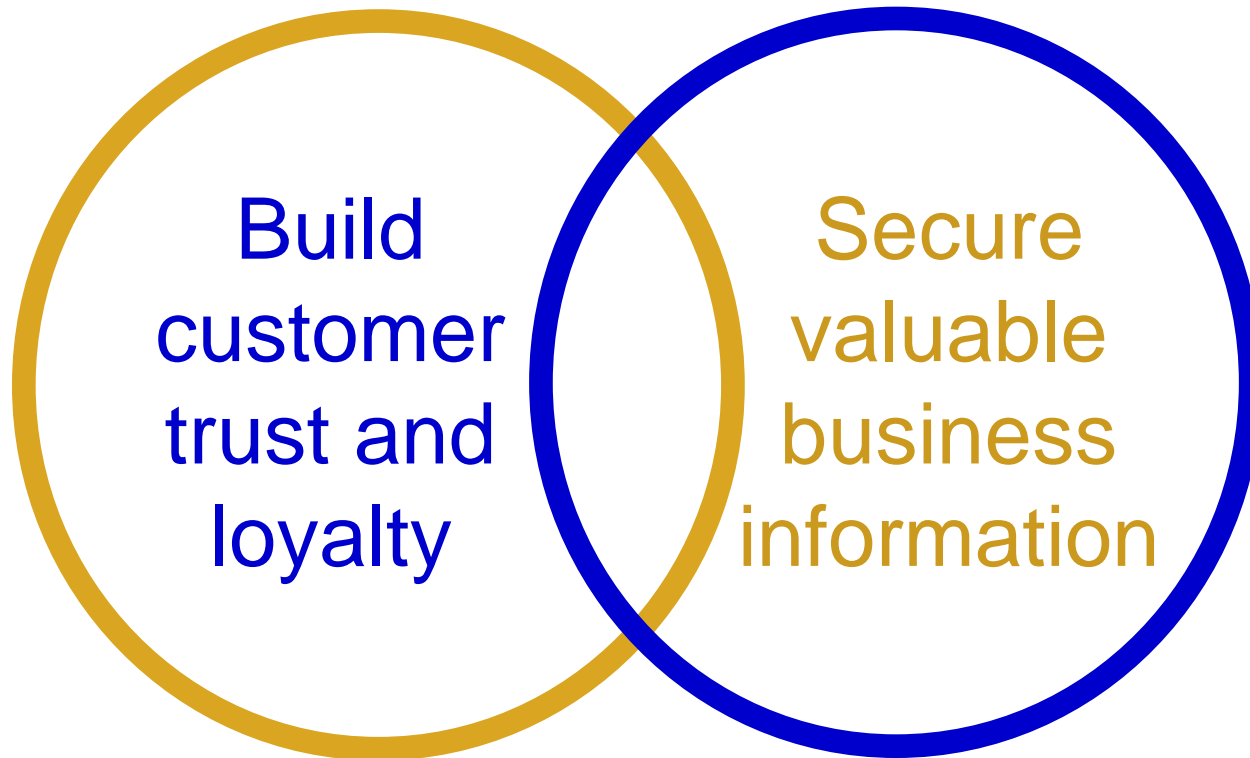
---

“Trust is the real currency of the Internet. Squander what you have and you’ll find out how hard it can be to get more.”

Scott McNealy, 2001

# Business Imperatives

---



Applied Privacy & Security Group

**APS**Group

For more information, to request a presentation to your organization, or for assistance with conducting an Opportunity and Risk Assessment, please contact us at:

**[Information@APS-Group.com](mailto:Information@APS-Group.com)**

Seminars and self-assessment tools are also available.