RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: CXO-RO2

CYBERSECURITY AND DATA BREACHES FROM A BUSINESS LAWYER'S PERSPECTIVE

Kathy Winger

Law Offices of Kathy Delaney Winger
@KathyDWinger

CASE STUDY: TARGET

Businesses have a duty to protect consumers and banks from the criminal conduct of third parties and are subject to claims for breaching that duty.

CASE STUDY: ALPINE BANK

Small companies are not immune from liability.

LESSONS LEARNED

- Risk of loss extends to almost everyone who does business.
- Others' costs of doing business are now your your costs of doing business.
- You may be held legally responsible for privacy violations or data breaches that occur as a result of your vendor's unreasonable security practices.
- ALL BEHAVIOR IS NOW SUBJECT TO SCRUTINY.

DISTURBING STATISTICS

More than 60% of data breaches occur at small and medium sized businesses.

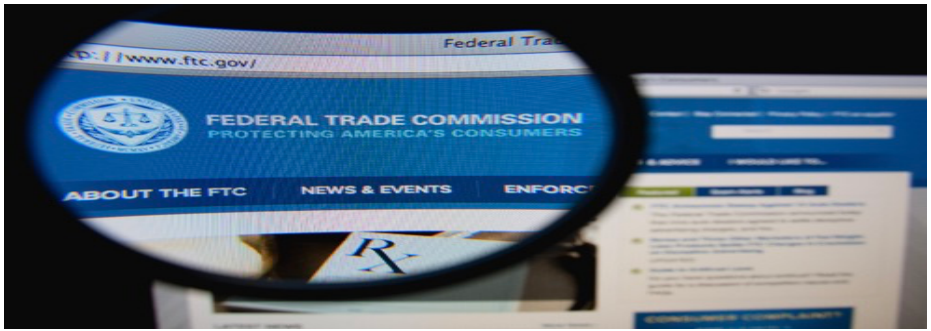
More than 50% of small businesses close their doors within 6 months of a data breach.

Liability for vendor's actions – What to do

- Same or better data security standards
- Understand how vendors handle and store information
- Vendor contracts:
  - Require vendors to follow practices to safeguard sensitive information and to protect privacy of your and your customers' information
  - Include indemnification clause
- Vendor certifies that it has cyber insurance coverage
- Ask to be added as an additional insured
- Vendor expectations/good security practices as a marketing tool

Commercially Reasonable Standard

- FTC applies standard when it investigates data security matters.
- Standard relevant from a security, legal and insurance perspective before, during and after a data breach.
- In practice, FTC applies cybersecurity “best practices” in a legal context.

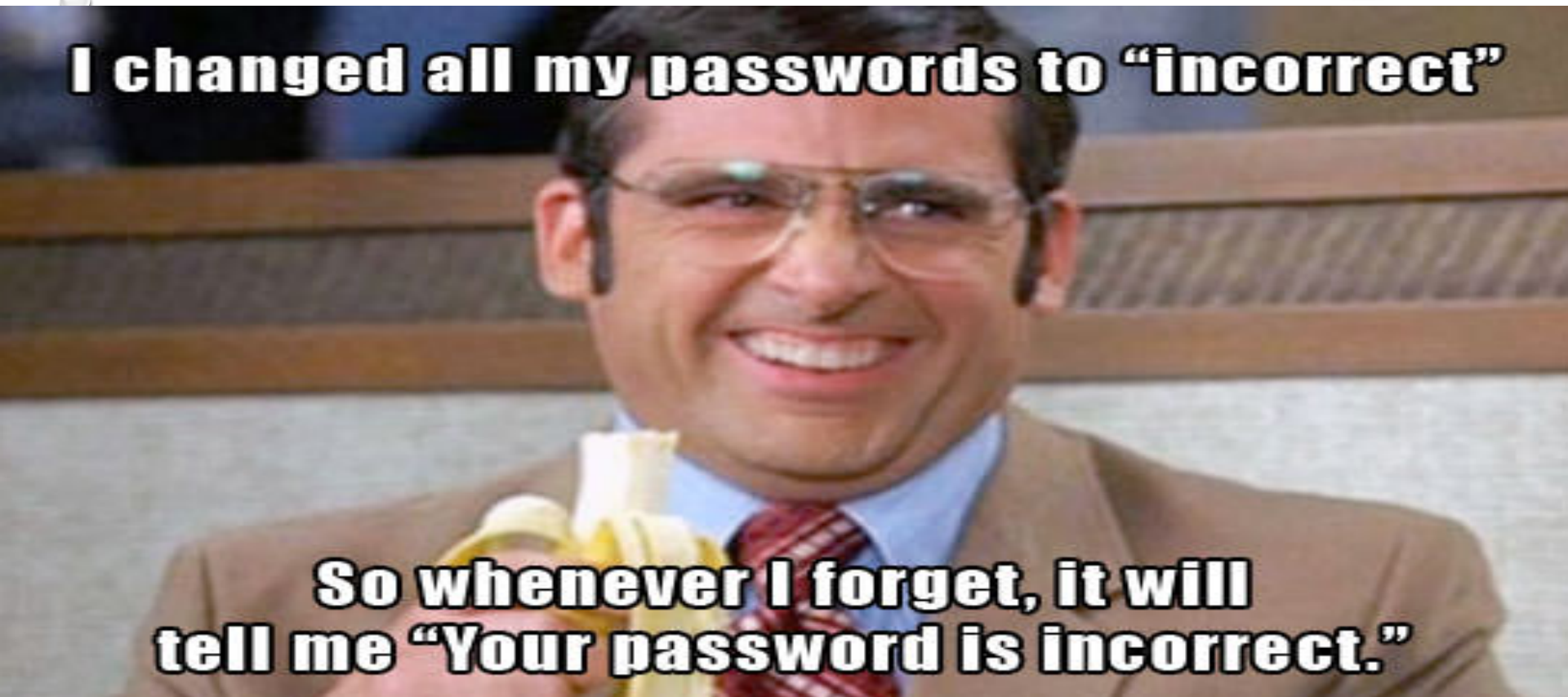


Unreasonable Practices (per the FTC)

- Not preventing access to network or restricting access to those with a need-to-know
- Not monitoring network to detect questionable activities or unauthorized users
- Ignoring warning signs of issues with your network or security warnings

Unreasonable practices (per the FTC)

- Violating industry (i.e., PCI DSS) standards
- Not maintaining and using up-to-date anti-virus software or using systems to protect against malware
- No written data breach response plan
- No employee training on data security

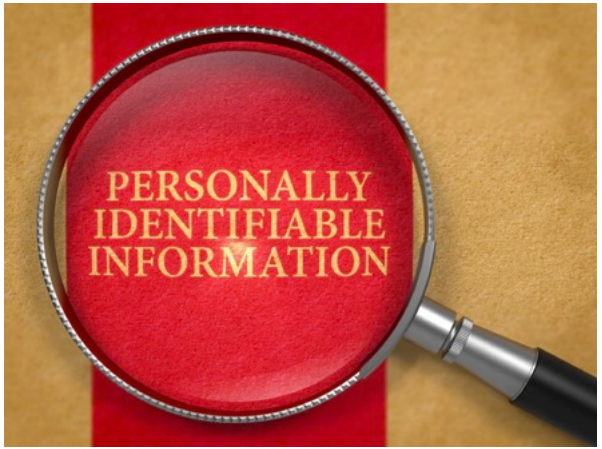

I changed all my passwords to “incorrect”
So whenever I forget, it will
tell me “Your password is incorrect.”

Cyber Insurance (Transferring Risk)

- Cyber liability generally excluded from property and general liability insurance.
- Cyber insurance doesn't eliminate the need to invest in cyber security.
- Link between cybersecurity practices and cyber insurance policies.

Cyber Insurance Questions

What type of data is covered (PII, PHI, PCI,…)?



Cyber Insurance Questions

- Does it matter where the data is stored?
- What is the trigger of coverage (claims made, claims made and reported or occurrence)?

Cyber Insurance Questions

- Does the policy cover:
  - Prior acts (e.g. hackers gain access to your network without your knowledge prior to the policy period)
  - Third parties (e.g. vendors)
  - Hardware replacement?

Cyber Insurance Questions

- Does the policy cover:
  - Software upgrades
  - Bodily injury (e.g. insulin pump failure)
  - PCI fines
  - Reputation damage?

Cyber Insurance Questions
What is a Covered Data Breach?

- Policy should cover:
  - Unauthorized (accidental or intentional) disclosure of data.
  - Unauthorized acquisition of data by third party.
  - Compromised data (corrupted, erased, altered or held for ransom).

Cyber Insurance Questions: Policy Limits

Are defense costs included in policy limits?

If so, the total amount of coverage may be eroded.

Cyber Insurance Questions: Policy Limits

- Are there sublimits for
  - Legal fees
  - Forensics
  - Public Relations Expenses
  - Crises Management Expenses?

- If so, make sure the amounts are sufficient.

Cyber Insurance Questions

- Does coverage for loss of business require a complete suspension of business operations or is an interruption in business operations sufficient – how long must business be interrupted?

- Does the the policy cover lost profits?

Cyber Insurance Pitfalls

- Policy precludes coverage for social engineering (e.g. business email compromises where employee negligently provides or is tricked into providing access).
  - If not under cyber, check commercial crime coverage.

Cyber Insurance Pitfalls

Canadian and US court decisions regarding social engineering coverage.

Cyber Insurance Pitfalls

- Policy precludes coverage where insured fails to follow minimum required security practices or best security practices.
- Policy precludes coverage for cyber attacks initiated by individuals or entities in foreign countries or foreign countries themselves.
- Directors & Officers coverage excludes cyber liability.

WATCH FOR LEGISLATION

NEW YORK DEPARTMENT OF FINANCIAL SERVICES CYBERSECURITY REGULATION

WATCH FOR LEGISLATION

EUROPEAN UNION GENERAL DATA PROTECTION REGULATION

FROM COURTS AND REGULATORS

- Ransomware attack may constitute a breach that requires notification.

- Business email compromise scams may not be covered by cyber insurance.
  - Rulings from Canadian and United States courts

FROM COURTS AND REGULATORS

- If it takes six weeks to announce a data breach, you've waited too long (NY DFS cybersecurity regulation and GDPR allow 72 hours).

- Involve competent privacy/data breach counsel in all post-breach actions and investigations.

CYBERSECURITY TIPS FOR BUSINESS OWNERS AND TECHNOLOGY PROFESSIONALS

- Start thinking about your cybersecurity and conduct your own risk assessment to determine the most important information and data your business holds.

- Have a written data breach plan in place so that you're ready before a breach occurs. Plan should:
  - Address how the company will respond to a breach
  - Establish a breach response team whose members are assigned specific responsibilities (e.g., IT response, law enforcement, public relations, customer issues, legal issues).

CYBERSECURITY TIPS FOR BUSINESS OWNERS AND TECHNOLOGY PROFESSIONALS

- Get at least three cyber insurance quotes and compare their different features and benefits.
- Take all necessary steps to ensure that your vendors have the same or better security standards than you and include those security requirements in your vendor agreements along with an indemnification clause and cyber insurance coverage certification.
- Ensure that employees are continuously trained about data security and equipped with best practices to avoid data breaches.