David Childers, CEO Compli
Vivek Krishnamurthy, Foley Hoag LLP

FOLEY HOAG

HCCA

compli cool, calm and compliant.™

Global Economic Crime Survey

- Global Cyber-Crime is the **fastest growing economic crime**
- Cyber-Crime is **more lucrative than trafficking drugs!**
- 60% of HCCA respondents' organizations had suffered an incident in the last year, and 20% had suffered four or more
  - Reputation damage was the greatest fear among the participants
  - Cost per breach averaged $50K with some greater than $200K
  - Human error and electronic exploitation split 50-50
    - Lost devices and improper paper handling are the leading culprits

Data Breach Incidents & Responses **- A 2012 Survey by SCCE and HCCA**

FOLEY HOAG

compli cool, calm and compliant.™

Data Breach Costs

$194 per record lost*

You do the math…

*Ponemon Institute, US Cost of Data Breach, 2012, and Reputation Impact of a Data Breach, Nov 2011

FOLEY HOAG

complí cool, calm and compliant.™

Data Breach Costs

- $194 per record lost*
  - You do the math…
- Collateral Damage
  - Brand Reputation
  - Share Price
  - Employee Morale
  - Business Relations

*Ponemon Institute, US Cost of Data Breach, 2012, and Reputation Impact of a Data Breach, Nov 2011

FOLEY HOAG

complí cool, calm and compliant.™

Causes of Cyber Attacks

Why Cybercrime?

- Economic Crime
- Espionage
- Activism
- Terrorism

Data is more valuable than money.

Once spent, money is gone, but data can be used and reused to produce more money.

The ability to reuse data to access on-line banking applications, authorize and activate credit cards, or access organization networks has enabled cyber criminals to create an extensive archive of data for ongoing illicit activities.

Cyber crime: A clear and present danger: Combating the fastest growing cyber security threat. Deloitte Center for Security & Privacy Solutions

FOLEY HOAG

complí cool, calm and compliant.™

Causes of Cyber Attacks

Why Cybercrime?

- Economic Crime
- Espionage
- Activism
- Terrorism

Who is the Internal Cybercrime Risk?

- **Junior employee or a middle manager**
- **Less than 40 years old**
- **Employed for less than 5 years**
- **Significant use of social media**
- **Often disgruntled**
- **Not as tech-savvy as s/he thinks**
- **Subject to employment agreement**
  (confidentiality, computer use policy)

FOLEY HOAG

complí cool, calm and compliant.™

Cyber Scenario

- You are the CCEO for a large organization with several thousand employees.
- The organization sells internationally and has hundreds of thousands of users
- You arrive at work and the office is buzzing; the CISO comes in to tell you that the company has experienced a DoS and that the systems are still down.
- All efforts with the ISP and internal resources have been ineffective

FOLEY HOAG

complí cool, calm and compliant.™

Cyber Scenario

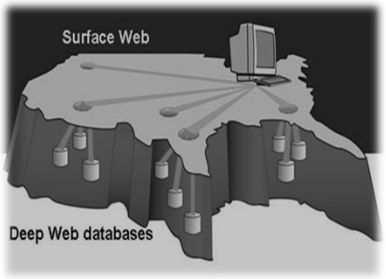
- At 9:30 you are called to a meeting with the CEO
- In the room are the CISO, CEO, CCEO and the CTO. The CTO shares the bad news that the DDoS was apparently a diversion and that the database had been hacked.
- The CEO asked how "bad" was the hack? The CTO tells the team that based on his early estimates as many as 400,000 user names, passwords and some PII could have been compromised.
- You ask when he will know the extent of the damage? He shares it will be a couple of days.

FOLEY HOAG

complí cool, calm and compliant.™

Cyber Scenario

- Later that afternoon the CISO gets a phone call from a friend of his from college that works for the NSA. He shares that about 1000 names and hashed passwords were posted on the deep web with a request for information on how to unencrypt the passwords. The hacker shared in his request that he had successfully hacked your company.
- The CEO calls another meeting and asked the team – **what do we do now?**



FOLEY HOAG

complí cool, calm and compliant.™

Just so you know…

- This is a scary scenario!
- It wasn't completely fictional…
  - **LinkedIn**
  - **Yahoo**
  - **Formspring**

All experienced something like this – in 2012!

FOLEY HOAG

complí cool, calm and compliant.™

In fact….

symantec.

NORTHROP GRUMMAN

RSA SECURITY™

NASA

VeriSign Secured

CENTRAL INTELLIGENCE AGENCY

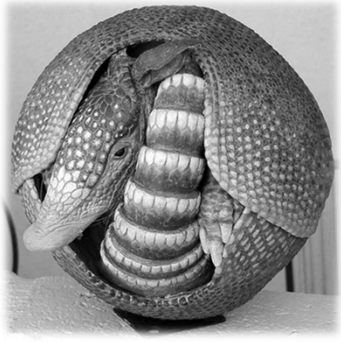
NEW SCOTLAND YARD LONDON

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

Cyber Governance – Means Cyber Vigilance

Traditional
Anti-Intrusion Defenses



Today's
Cyber Warfare Tools

FOLEY HOAG

complí cool, calm and compliant.™

Cyber Intelligence

- Establish the appropriate cyber threat awareness
  - Understand your cyber risks
  - Include 3rd Party data processors
  - Know your cyber neighbors
  - Know which data repositories contain actionable PII
- Create a mechanism to constantly review the changing cyber landscape
  - Develop and implement cyber incident response protocols and procedures
  - Conduct periodic testing and mock "drills" to ensure the effectiveness of information security policies and data loss procedures
  - What new technologies do we need to watch and/or monitor?
- Communicate up and down the chain of command
  - Tone at the top
  - Mood in the middle
  - Buzz at the bottom

FOLEY HOAG

complí cool, calm and compliant.™

Federal Regulatory Risk

Relevant to data breaches involving federally protected information

- Education Information (FERPA)
- Financial Information (EFTA, FCRA)
- Health Information (HIPPA)
- Personal Communications (ECPA, SCA, Wiretap Act)
- Any other Identifiable, non-public information (GLBA)

FOLEY HOAG

complí cool, calm and compliant.™

Federal Regulatory Risk

- Remedies for Breach Victims
  - Private Rights of Action
  - Government-imposed fines (up to $1.5M under HIPPA)
  - FTC injunctions, reporting, and standards
- Remedies for your company
  - Federal law enforcement investigative assistance
  - Temporary and permanent remedies from federal courts
  - Executive Branch assistance in international incidents

FOLEY HOAG

complí cool, calm and compliant.™

State Regulatory Risk

- A regulatory patchwork with some common themes:
  - Generally protect non-public information ("NPI")
  - Often impose physical and technical data security standards (encryption in Massachusetts)
  - Generally require breach notification
- State cyber-security laws are evolving rapidly
- State laws may apply across state lines
- State law provides most remedies for internal breaches (breach of contract, tort law)

FOLEY HOAG

complí cool, calm and compliant.™

Foreign Regulatory Risk

- More and more international jurisdictions are passing cyber-privacy and security laws
- Foreign laws often impose stricter requirements than U.S. laws ➔ a race to the top?
- Foreign operations subject your company to foreign regulation
- Foreign laws may not always provide effective legal remedies against breaches

FOLEY HOAG

complí cool, calm and compliant.™

Key Questions that should be asked…

- How many records are affected?
- Who alerted us to the breach?
- Was the breach malicious or accidental?
- When did it occur?
- What is the quality of the data?
  - Was PII involved
- Was it encrypted?
- What is the expected impact?
- What press coverage impact should we expect?

FOLEY HOAG

complí cool, calm and compliant.™

Breach Response Best Practices

- Prior to a breach, establish a breach response team with clear roles.
- Make sure you have all the facts before you reveal information about the breach to those impacted.
- Engage outside expertise early to determine which steps to take and the laws that must be complied with.
- Talk with counsel before alerting authorities or outside agencies; once they are involved your best interests become less important.
- Notify the appropriate authorities (federal/state/local law enforcement and regulators)

FOLEY HOAG

complí cool, calm and compliant.™

Breach Response Best Practices

- Do not put the CEO in front of press too early or lead with a message that the breach is “no big deal”.
- Is the organization at risk of legal action?
- Be a transparent as possible with the breached population. They will forgive you for being hacked, but not for holding back the truth.
- Understand any data breach or cyber liability insurance that your company may have in place, and if there is coverage, notify your insurer early.
- Exercise a consistent communication strategy directed at <u>everyone</u> in the company.

FOLEY HOAG

complí cool, calm and compliant.™

Breach Response Best Practices

- The risk of legal action is high, assume you will need to defend your response in court
  - Keep the proper documentation of your decisions throughout the response process
- Preserve evidence of breach for investigation
  - Segregate affected computers, hard drives, etc.
  - Hire data forensics firm to conduct breach analysis
  - Hire computer security firm to audit network and security infrastructure
- If an internal breach is suspected, re-screen key employees for cyber-breach risk factors
  - Divorce, catastrophic illness, financial distress, etc.
- Don't take retaliatory counter-measures against cyber-criminals: these may violate federal law
- Consider filing for emergency judicial relief (e.g. injunction against disclosure of trade secrets)

FOLEY HOAG

complí cool, calm and compliant.™

Thank You!

David Childers – david.childers@compli.com

Vivek Krishnamurthy - vkrishnamurthy@foleyhoag.com

FOLEY HOAG

HCCA

complí cool, calm and compliant.™