CSO PERSPECTIVES

CSO Perspectives on
Defending Against the Pervasive Attacker

A Regional Seminar

What to Do - and Not to Do - When Attacked: A Moderated Workshop

Nick Akerman

Partner

Dorsey & Whitney LLP

Joan Goodchild

Editor

CSO

You've Been Hacked

- You work for the Insomniac Mattress Company and have taken your first well-deserved vacation in the Caribbean.
- You are stretched out on the beach when the company's CEO calls you on your cellphone and tells you someone may have hacked into his computer and stolen the company's super secret formula for creating its wildly successful mattress that instantly causes sleep when a person lies down on it.
- The secret formula was kept in a special computer in the CEO's office to which only several employees had the password including his former trusted assistant Sneaky Sam.
- Sam recently left the company as a result of a falling out with the CEO over his meager pay raise.
- Sam had at one point downloaded the formula to his new iPad, but no one knows if it was still on the iPad when he left the company.
- The secret formula has suddenly appeared on various Do-It-Yourself sites all across the Web.
- To make matters worse, the CEO also explained that the same computer contained the company's special list of high-end worldwide customers who charged their mattress purchases on Platinum American Express cards.

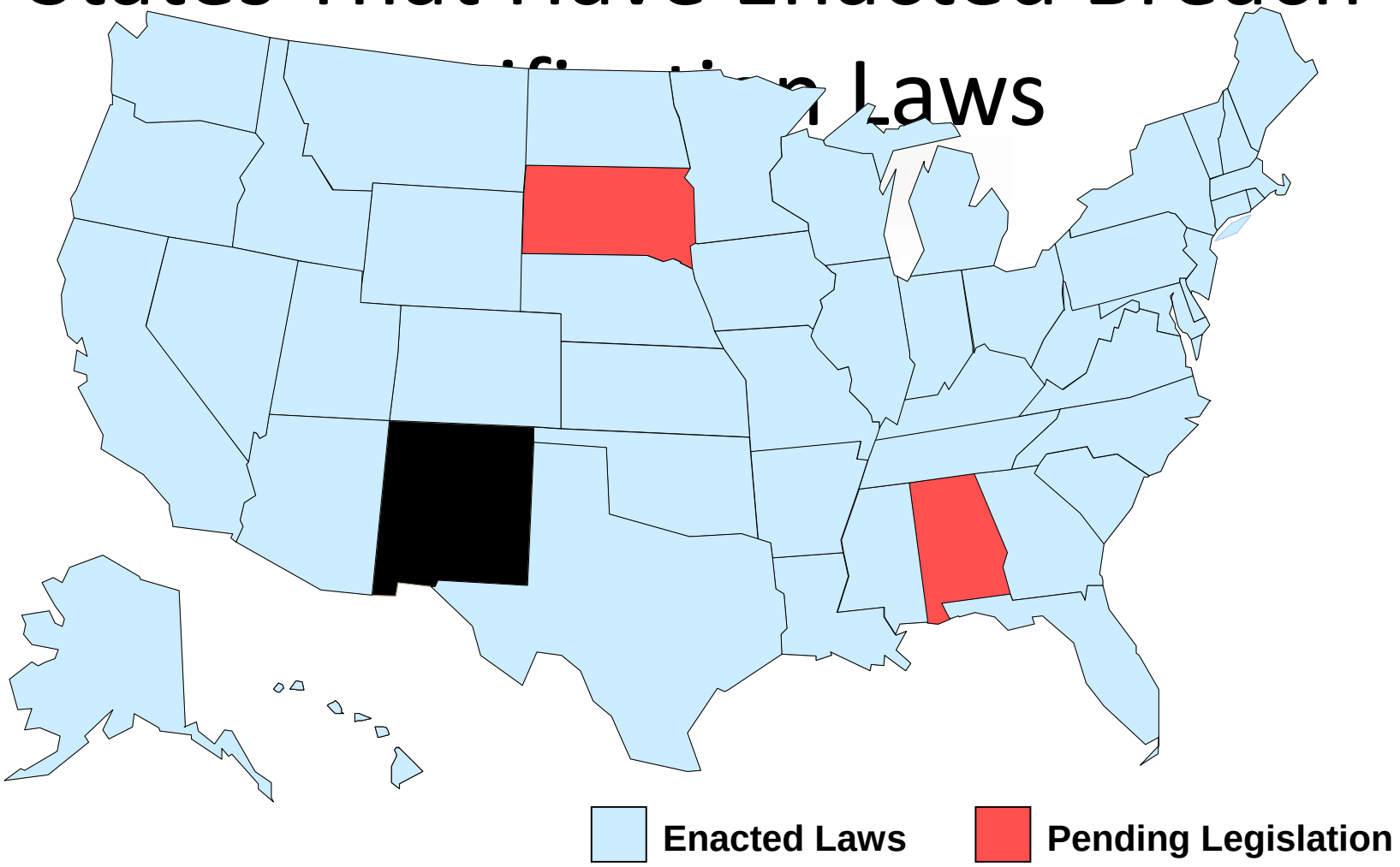
Insider Threat

- What do you do?
- Was it Sam or was it another insider?
- What's the potential damage?
- How do you respond?
- What do you do with Sam or another insider if you catch him/her?
- What are your legal options?
- Do you have to be concerned about creating any legal liabilities for the company?

Need for Advance Preparation

- Immediate action required
  - State breach notification laws
  - Injunctive relief in court
  - Retrieving stolen data
  - Federal Trade Commission
  - Securities & Exchange Commission
- Have a response plan in place

States That Have Enacted Breach Laws



Who Is the Response Team?

- IT Security
- Legal
- HR
- Compliance
- Risk Management
- PR

The Investigation

- Is there a Breach?
- What data was breached?
- What was the source of the breach?
- Inside or Outside?
- What can be done to secure the network?
- Document actions

Should IT Investigate?

- Perils of internal investigation
  - Destruction of Evidence
  - Lack of focus on admissible evidence
  - Legality of investigative techniques
  - Lack of coordination outside IT
  - Insider v. Outside attack

Involve Law Enforcement?

- Advantages
  - Breach may relate to bigger picture
  - Tools only government has
  - Some states require it
  - Increases timing on notification
  - Public relations
- Disadvantages
  - No guarantee of action
  - Loss of Control

Self Help Option: Computer Fraud and Abuse Act

- Title 18 U.S.C. § 1030 – Enacted in 1984
- Federal computer crime statute including data theft
- Civil remedy in 1994 amendment
- Computers used in interstate commerce
- Amended in 2001 and 2008
- Computers in foreign countries
- Provides for damages and injunction

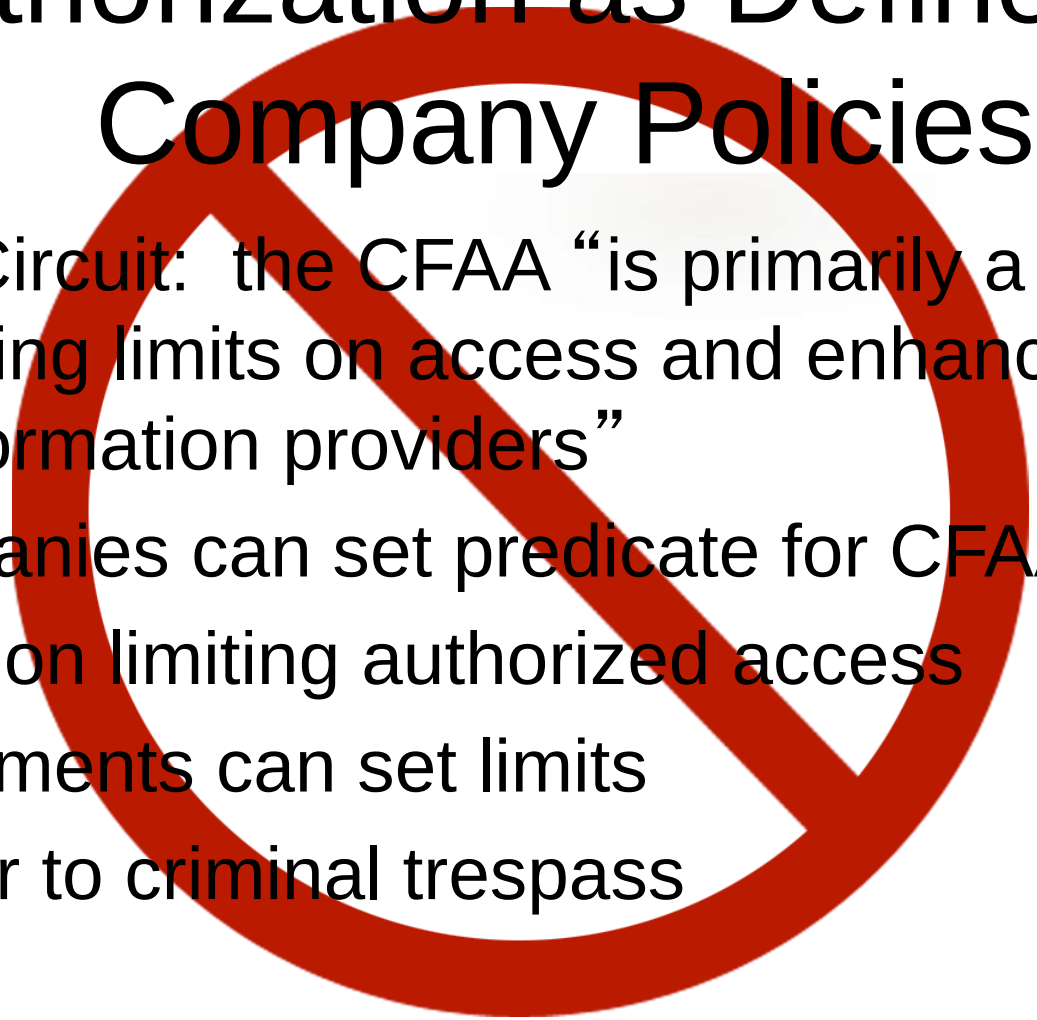
Legal Requirements

- ☑ Protected computer
- ☑ Lack of authorization or exceeding authorization to access computer
- ☑ Theft of information or anything of value
- ☑ Damage to data permanent
- ☑ $5,000 loss
- ☑ Limited to economic damages
- ☑ Compensatory damages

Policies

- How could this incident have been prevented or minimized through proper policies?
- What general computer policies need to be considered or created?
- How could proper policies have facilitated your ability to investigate? use the courts?

Authorization as Defined by Company Policies



- First Circuit: the CFAA "is primarily a statute imposing limits on access and enhancing control by information providers"
- Companies can set predicate for CFAA violation
- Rules on limiting authorized access
- Agreements can set limits
- Similar to criminal trespass

Company Rules

- Employee Handbook
- Compliance Code of Conduct
- Terms of Use on company Web site
- Training
- International rules

Agreements

- Define scope of authorized access to company computers
- Confidentiality/Non-Disclosure Agreements
- Officers/Employees/Customers
- Among related companies
- Post employment restrictive covenants
- Anti-Raiding Covenants
- Customer agreements
- Data vendor agreements

Compliance

- Trend is to be proactive as opposed to reactive
- Massachusetts Regulation
- Requires 7 steps of Effective Compliance Program per the Federal Sentencing Guidelines
- New York Stock Exchange listed company compliance program must protect confidential information that “might be of use to competitors, or harmful to the company or its customers, if disclosed.”
- Cover competitively sensitive data and personal data

The Nation-State Threat

- Rather than discovering your confidential information on the Internet, a forensic examination during an eDiscovery process has found what appears to be an intrusion of a very advanced level which has been systematically mining IP data from Insomniac Mattress' network over the past year and exfiltrating it to a location in an East Asian nation.
- Consultants you hired believe the source of the attack is indeed state-sponsored.
- How do you respond and why?
- Can you retaliate?
- Who is involved in the assessment of your response?

The Hacktivist Threat

- Rather than learning that your information is appearing on the Internet, word of the attack came from Special Agent Metz at the local FBI Office telephoned Insomniac's CEO.
- Agent Metz informed the CEO that the Bureau has an investigation based in Miami involving an Anonymous-like hacktivist group and there is reason to believe this group may have hacked into Insomniac's computer network.
- Agent Metz explains that because of government cutbacks, the FBI does not have the resources to investigate every lead coming out of this Miami investigation and is simply letting Insomniac know there may be a problem.
- The threats are unclear but, given the history of the hacktivist group, you are rightly concerned. What do you do? How do you prepare?