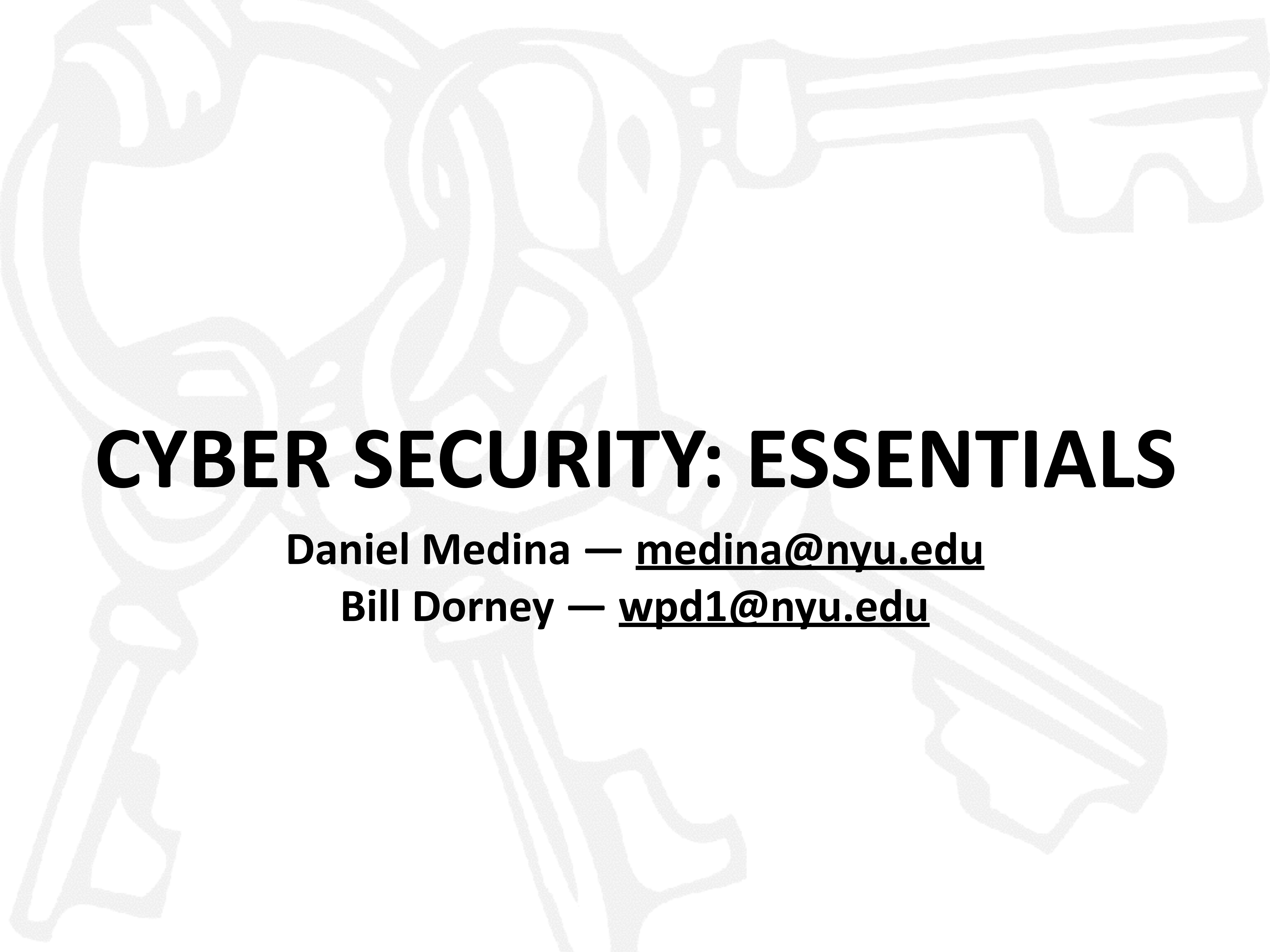


CYBER SECURITY: ESSENTIALS

Daniel Medina — medina@nyu.edu
Bill Dorney — wpd1@nyu.edu

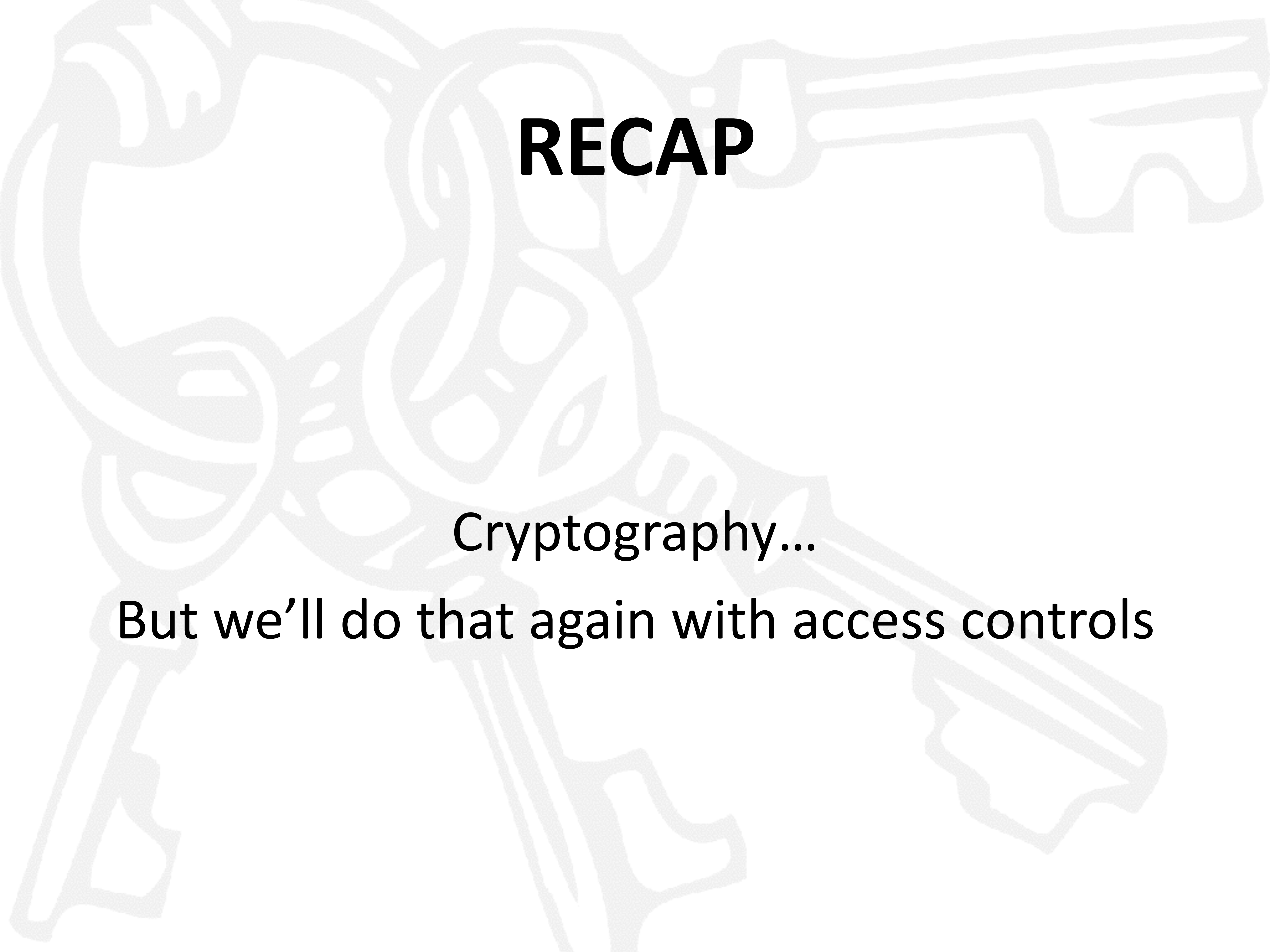
ADMINISTRATION

Need to reschedule missed class.

Re-ordering of classes (RSA Conference)

NEWS

Anything in the news?

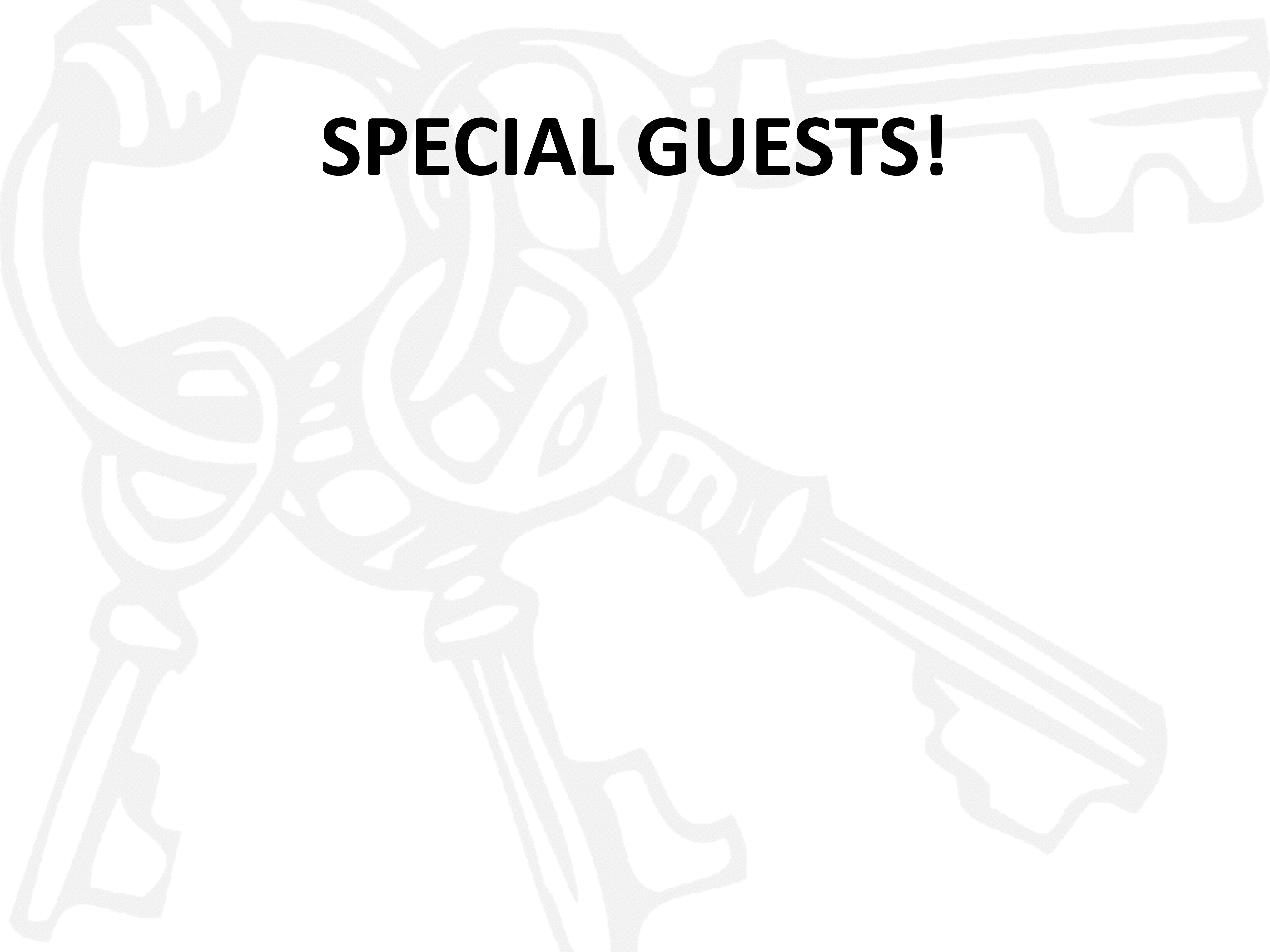


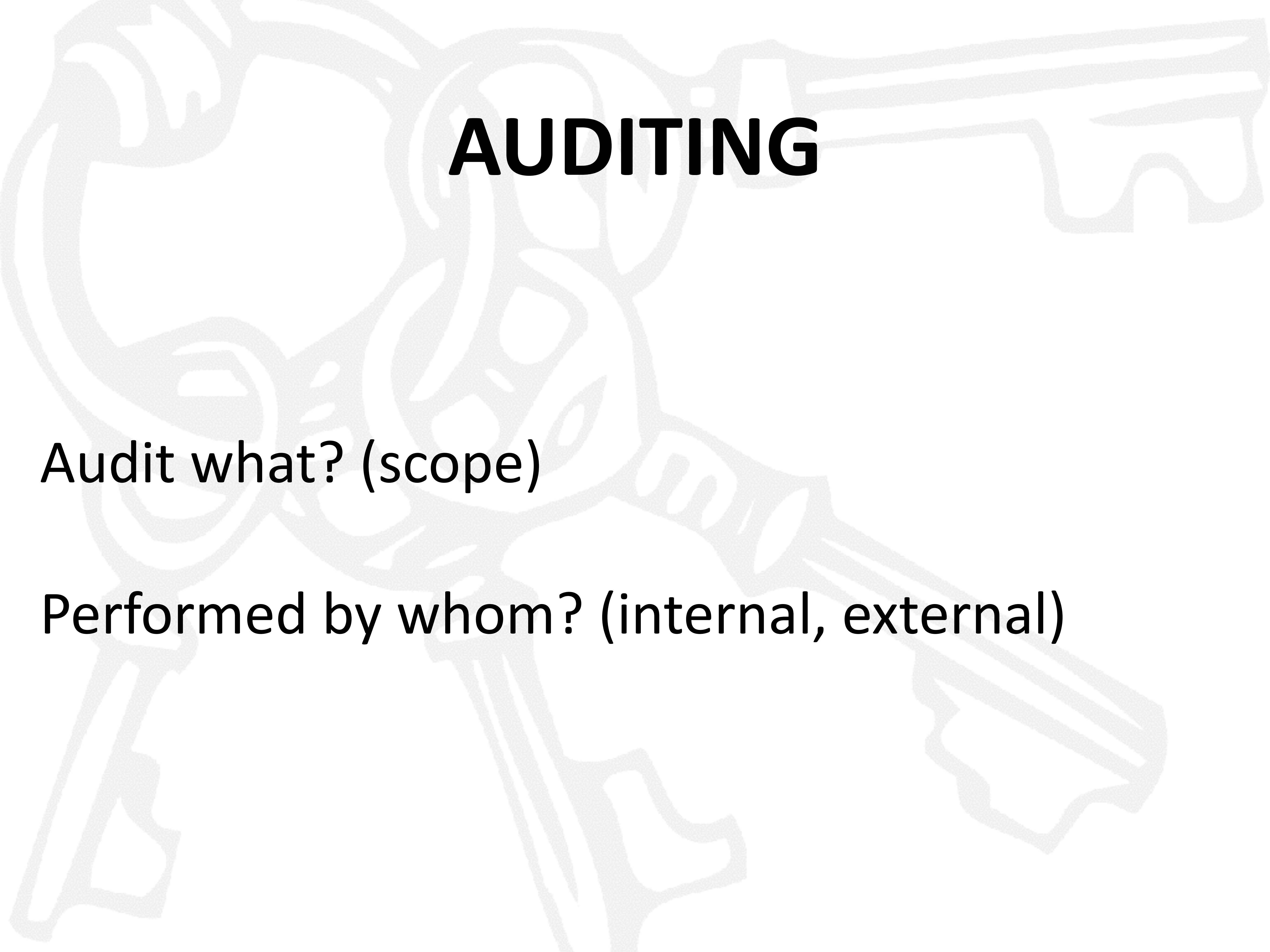
RECAP

Cryptography…

But we’ll do that again with access controls

SPECIAL GUESTS!



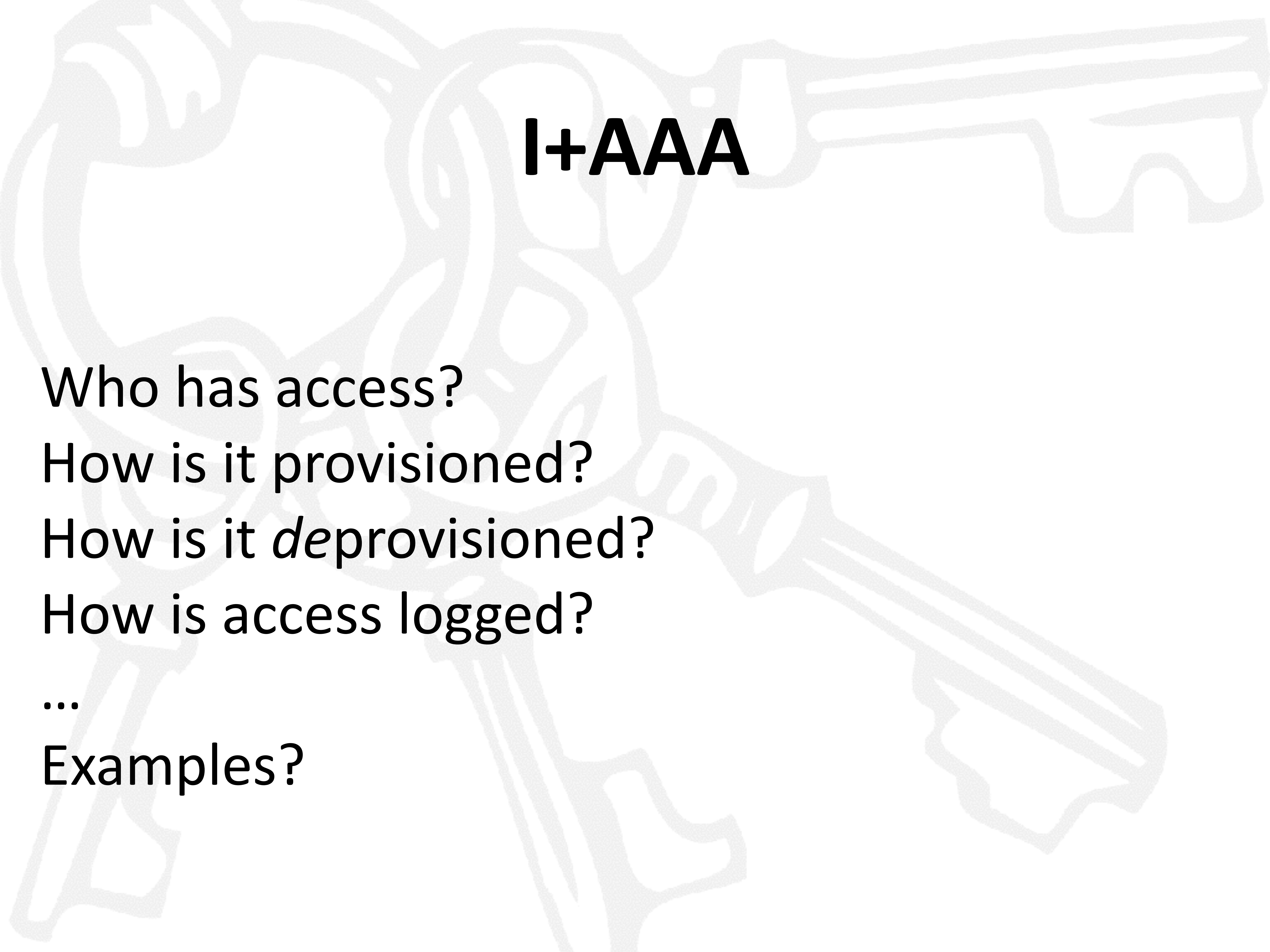


AUDITING

Audit what? (scope)

Performed by whom? (internal, external)

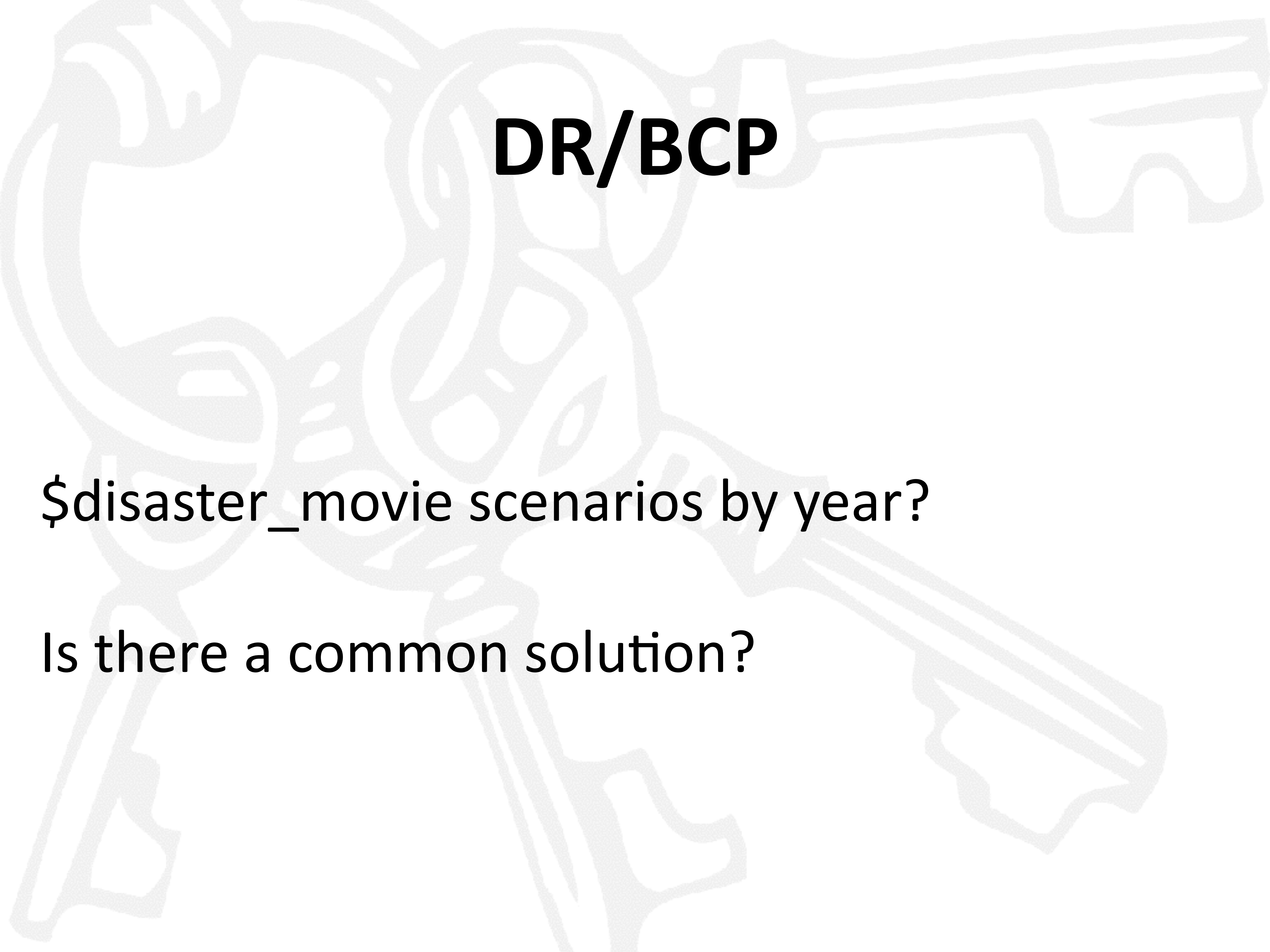
I+AAA



Who has access?
How is it provisioned?
How is it *de*provisioned?
How is access logged?
…
Examples?

DR/BCP

Do you have backups?
Can you restore from backups?
What is your plan for *$latest_disaster_movie*?
How often to you exercise your disaster plan?
…
Examples?

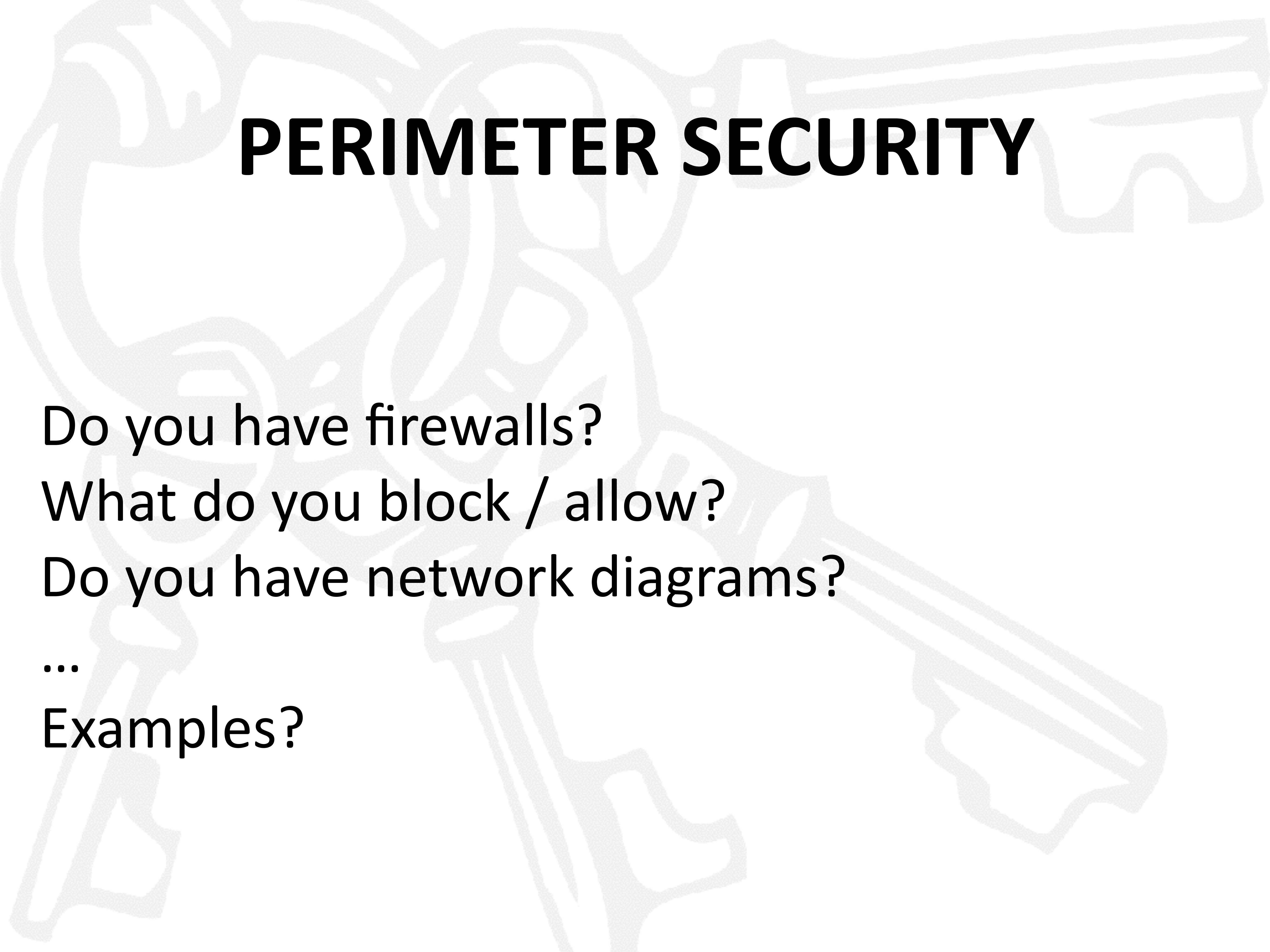


DR/BCP

$disaster_movie scenarios by year?

Is there a common solution?

PERIMETER SECURITY



Do you have firewalls?
What do you block / allow?
Do you have network diagrams?
…
Examples?

VULNERABILITY MANAGEMENT

Do you have an asset inventory?
Do you know what version systems are at?
Are your assets under support contract?
How what is your patching strategy?
…
Examples?

LOGGING AND INCIDENTS

Similar to I+AAA…

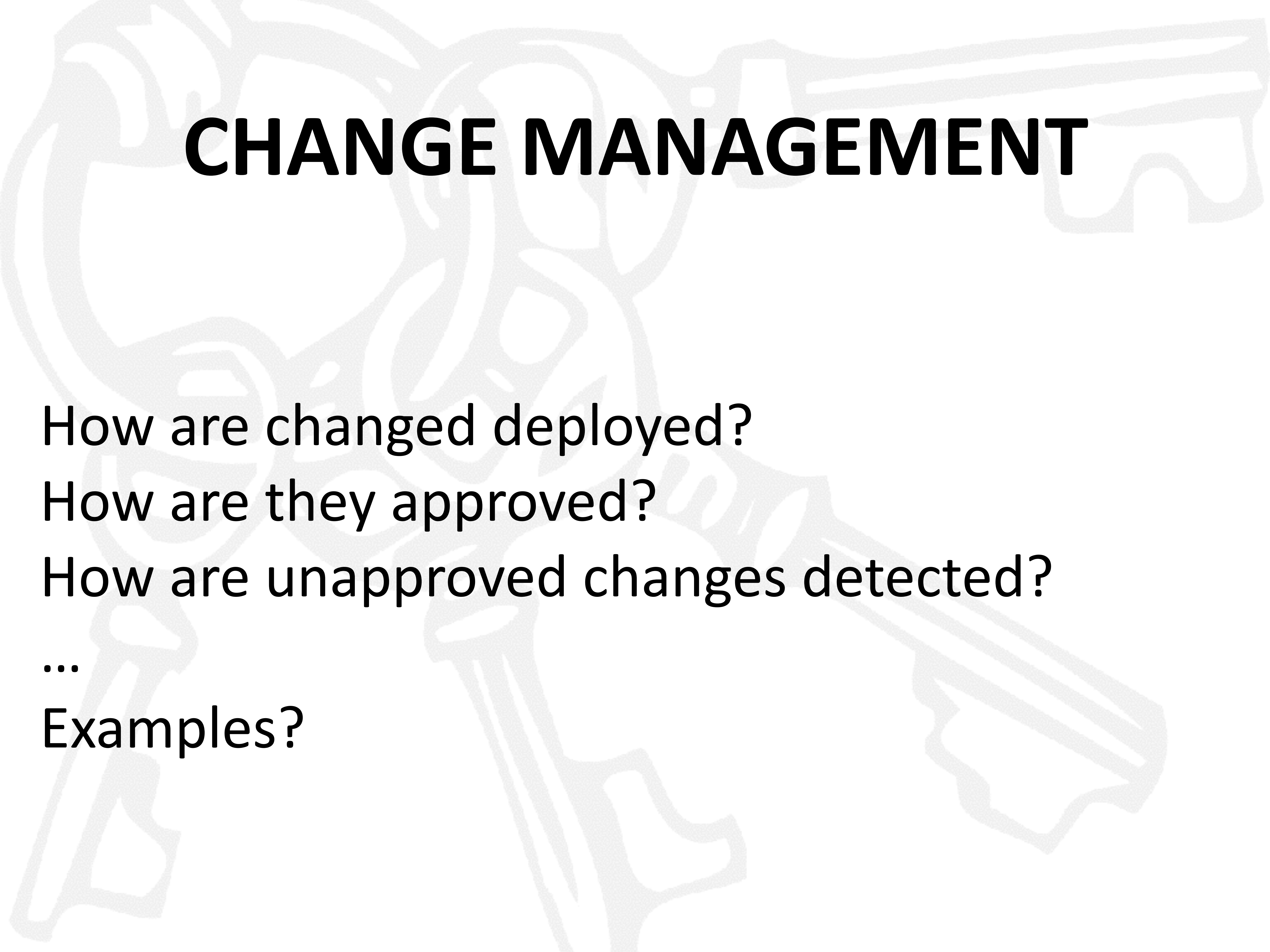
Do you log *security events*?

What action is taken in response to an event?

Do you have sufficient data retained?

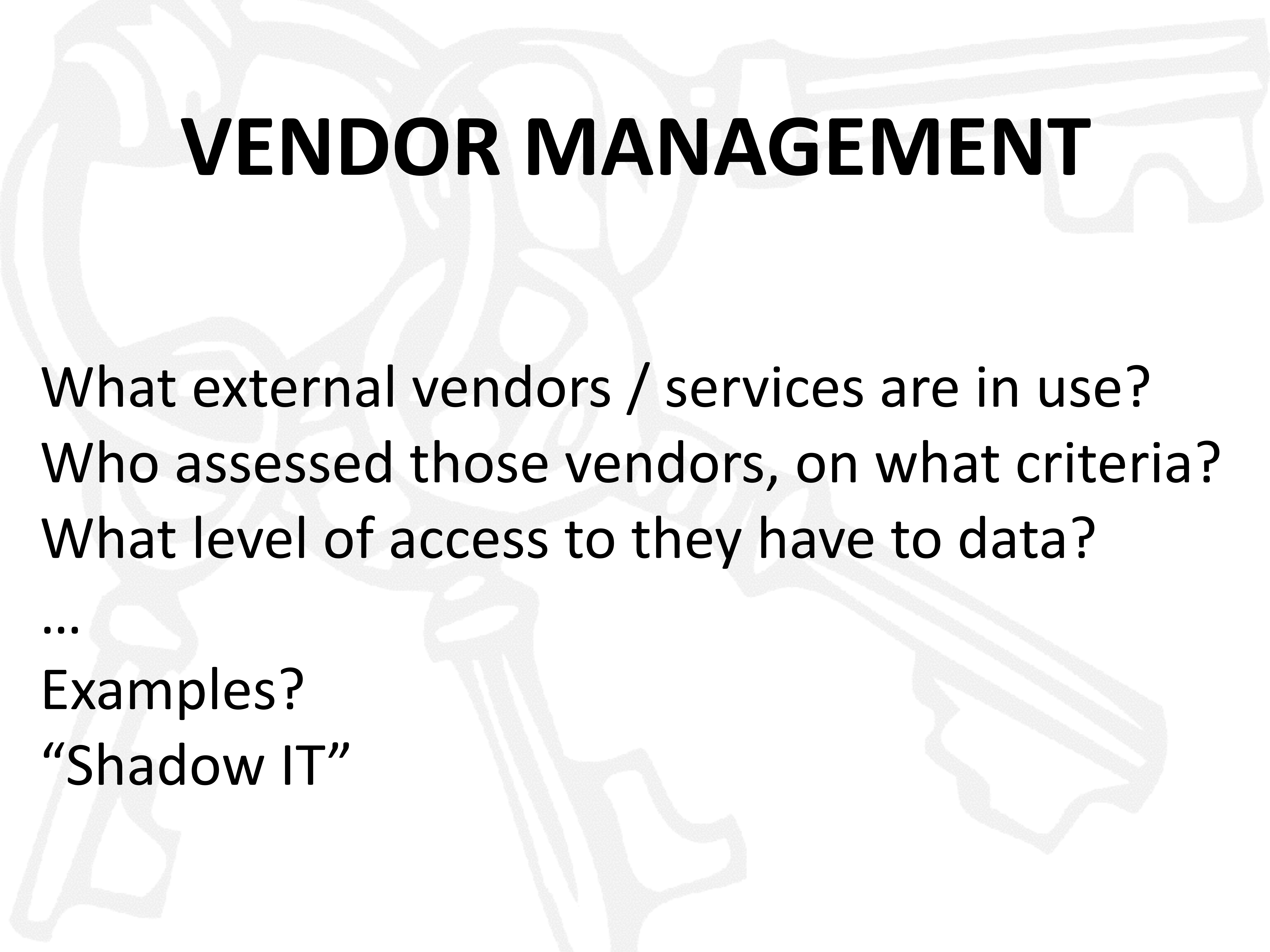
…

Examples?



CHANGE MANAGEMENT

How are changed deployed?
How are they approved?
How are unapproved changes detected?
…
Examples?



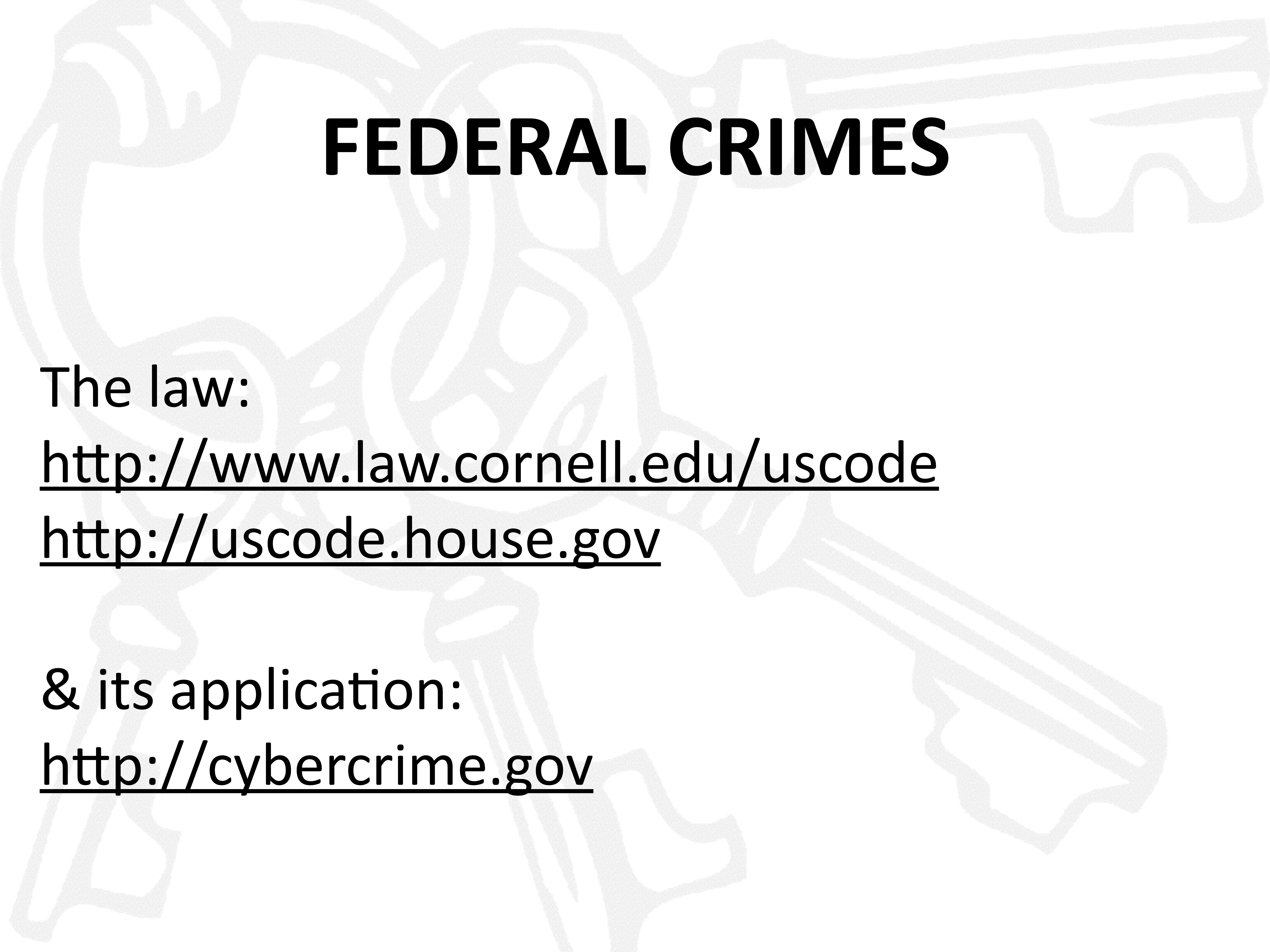
VENDOR MANAGEMENT

What external vendors / services are in use?
Who assessed those vendors, on what criteria?
What level of access to they have to data?
…
Examples?
“Shadow IT”

OTHER?

LAWS & REGULATIONS

FEDERAL CRIMES



The law:
http://www.law.cornell.edu/uscode
http://uscode.house.gov

& its application:
http://cybercrime.gov

18 USC 1030

Computer Fraud & Abuse
1986, 1994, 1996, 2001, …

Originally about “hackers”

Like this guy ->

18 USC 2511

Wiretap (aka Title III)
1968, 1986, …

Protects privacy of live communication

Service providers exemption for actions in the "normal course" of business.

18 USC 2701

Stored Communications

Applies to intentional, unauthorized access whereby the offender *obtains, alters, or prevents authorized access to a wire or electronic communication*

General exemption for service providers

EXAMPLES

Stakkato / FBI Case 216

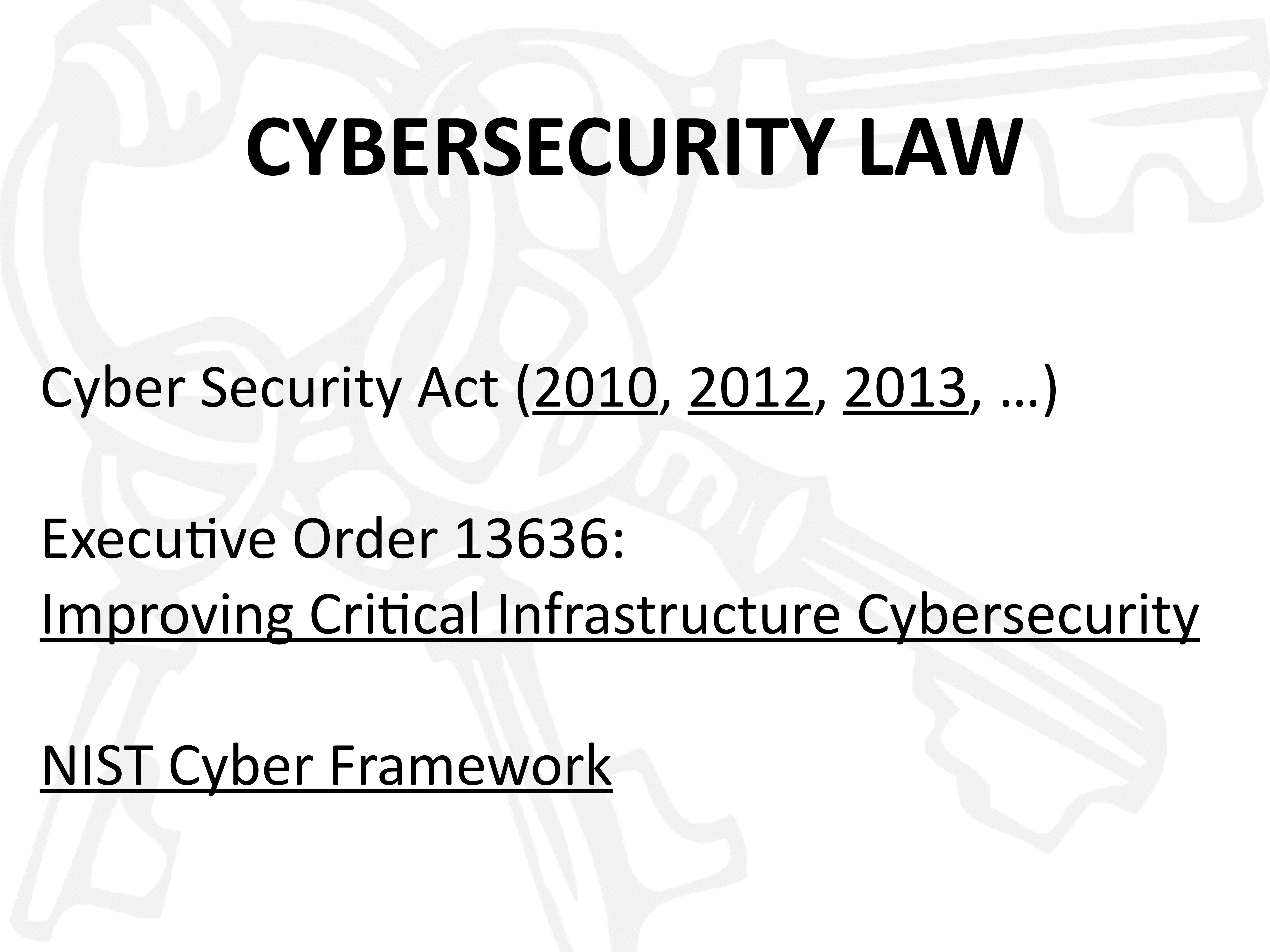
Weev / ATT (CFAA)

TJX / Gonzalez (CFAA)

Spammers (CAN SPAM)

US v Councilman (SCA)

Goldman "Code Theft"



CYBERSECURITY LAW

Cyber Security Act (2010, 2012, 2013, …)

Executive Order 13636:
Improving Critical Infrastructure Cybersecurity

NIST Cyber Framework

OTHER LAWS AND REGS

Family Educational Rights and Privacy Act (FERPA)

Health Insurance Portability & Accountability (HIPAA)

Gramm-Leach-Bliley Act (GLBA)

Sarbanes-Oxley Act (SOX)

State Privacy Laws: California SB 1386

Communications Assistance for Law Enforcement Act (CALEA)

EXTERNAL REQUIREMENTS

PCI DSS: Payment Card Industry

SEC Rules: e.g., Data Retention (Rule 204-2)

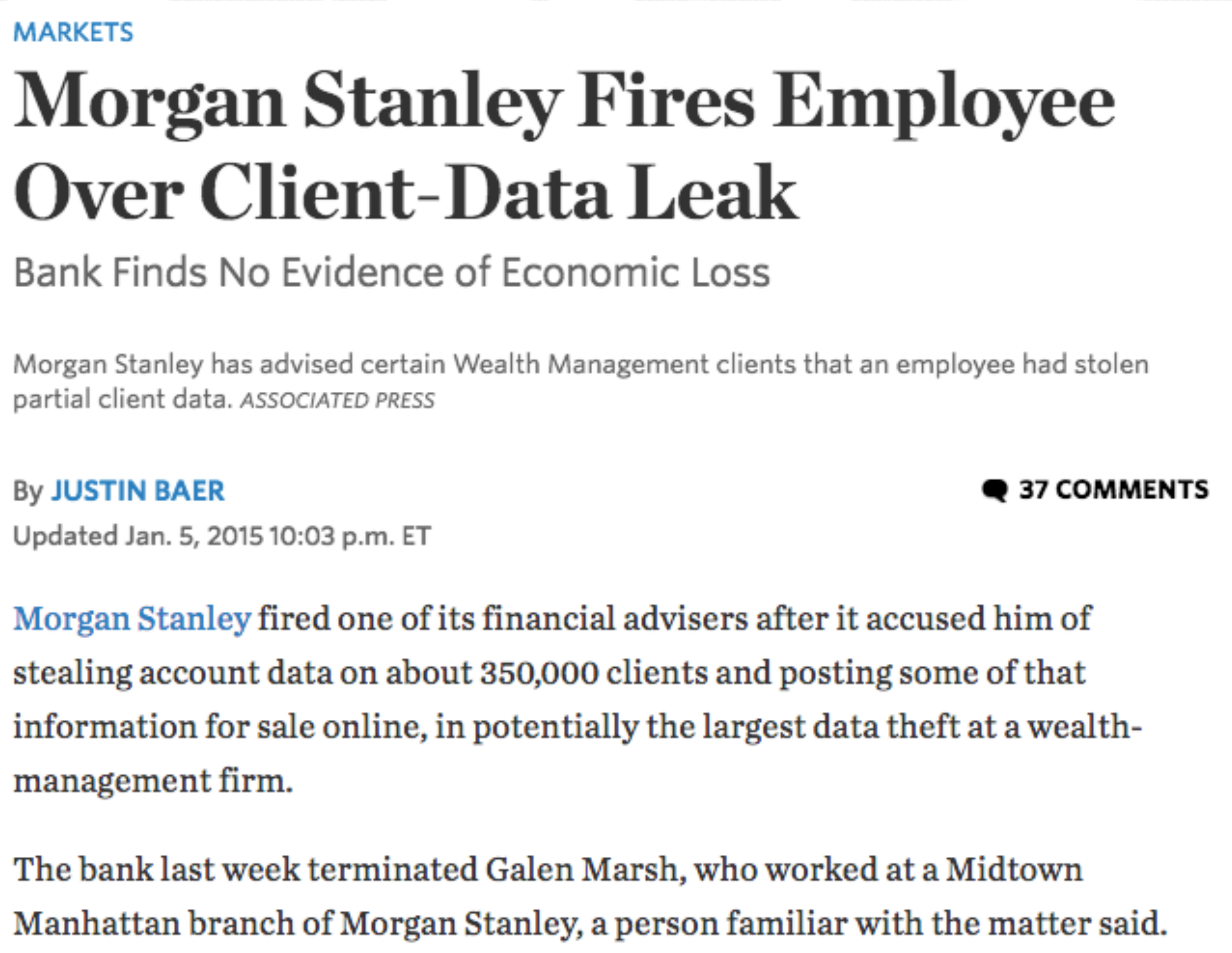
FFIEC Guidelines: e.g., Authentication

FTC Pseudo-Regulatory Framework: e.g., FB

REGULATIONS AS “MOAT”

https://aws.amazon.com/compliance/
https://azure.microsoft.com/support/trust-center/

Have a reg requirement to meet?
They meet ‘em all.
What about their competitors?



MARKETS

Morgan Stanley Fires Employee Over Client-Data Leak

Bank Finds No Evidence of Economic Loss

Morgan Stanley has advised certain Wealth Management clients that an employee had stolen partial client data. *ASSOCIATED PRESS*

By JUSTIN BAER

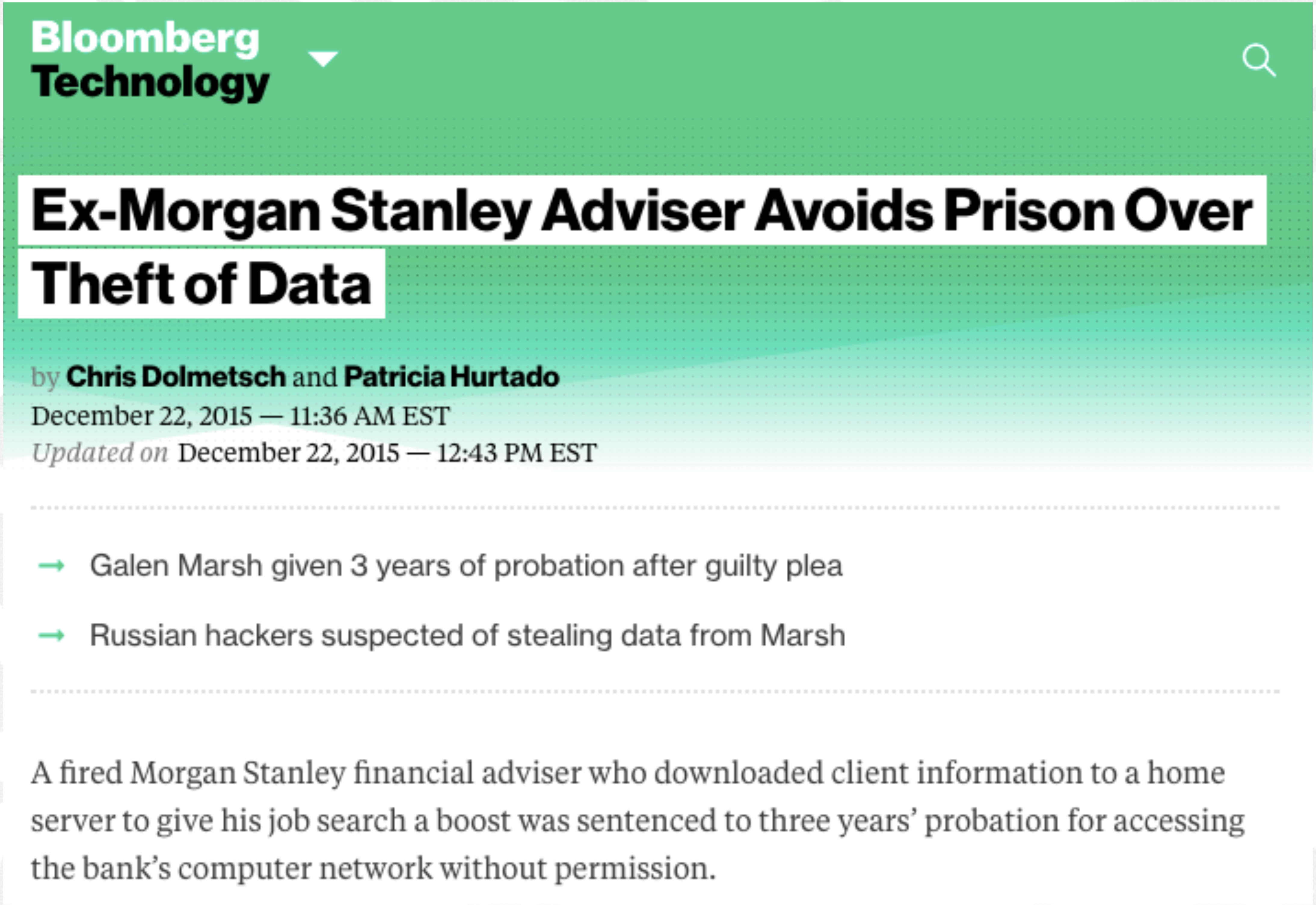
37 COMMENTS

Updated Jan. 5, 2015 10:03 p.m. ET

Morgan Stanley fired one of its financial advisers after it accused him of stealing account data on about 350,000 clients and posting some of that information for sale online, in potentially the largest data theft at a wealth-management firm.

The bank last week terminated Galen Marsh, who worked at a Midtown Manhattan branch of Morgan Stanley, a person familiar with the matter said.

http://www.wsj.com/articles/morgan-stanley-terminates-employee-for-stealing-client-data-1420474557



Bloomberg Technology

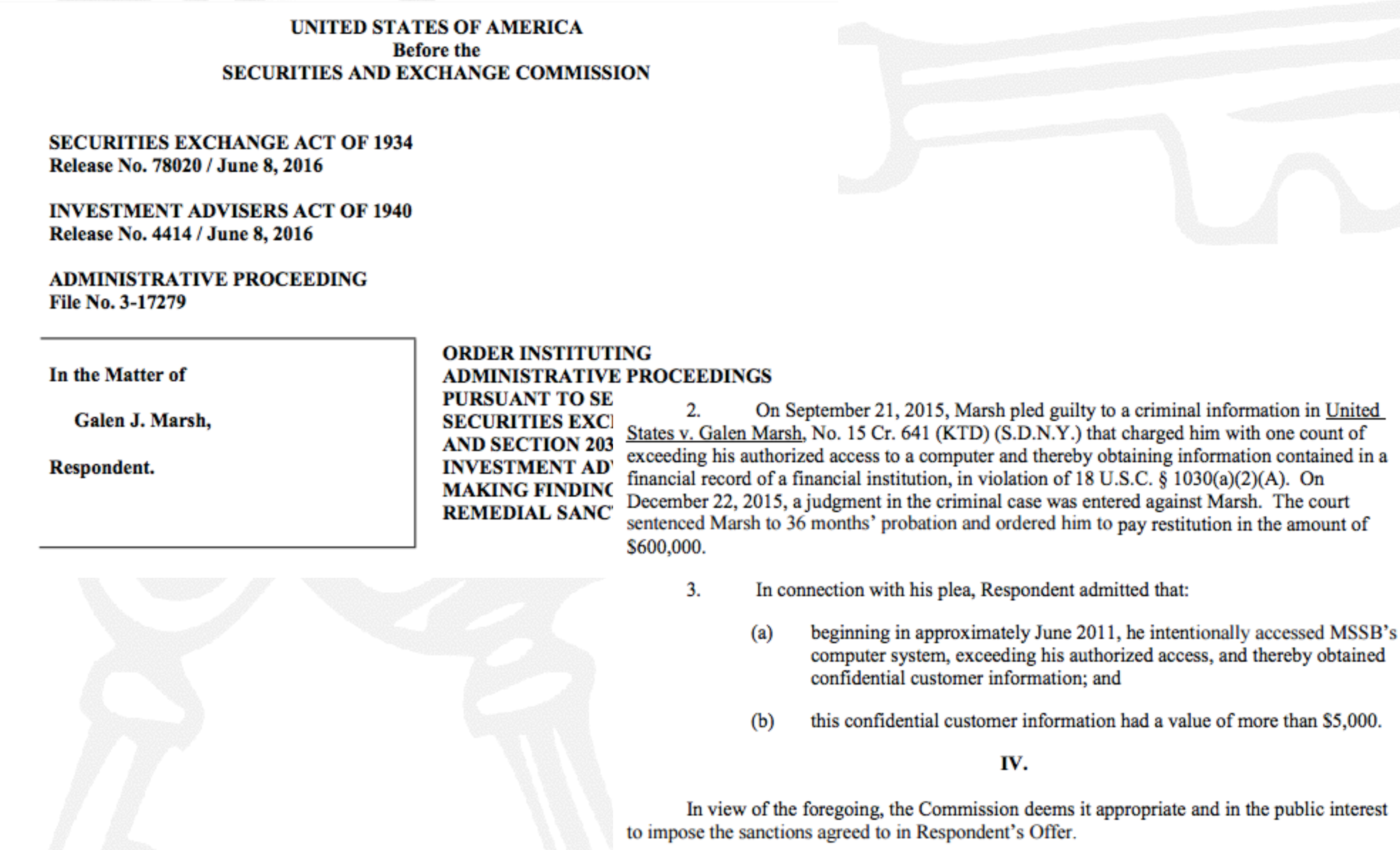
Ex-Morgan Stanley Adviser Avoids Prison Over Theft of Data

by **Chris Dolmetsch** and **Patricia Hurtado**
December 22, 2015 — 11:36 AM EST
Updated on December 22, 2015 — 12:43 PM EST

- → Galen Marsh given 3 years of probation after guilty plea
- → Russian hackers suspected of stealing data from Marsh

A fired Morgan Stanley financial adviser who downloaded client information to a home server to give his job search a boost was sentenced to three years' probation for accessing the bank's computer network without permission.

https://www.bloomberg.com/news/articles/2015-12-22/ex-morgan-stanley-adviser-gets-3-years-probation-for-data-theft



UNITED STATES OF AMERICA
Before the
SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 78020 / June 8, 2016

INVESTMENT ADVISERS ACT OF 1940
Release No. 4414 / June 8, 2016

ADMINISTRATIVE PROCEEDING
File No. 3-17279

In the Matter of

Galen J. Marsh,

Respondent.

ORDER INSTITUTING
ADMINISTRATIVE PROCEEDINGS
PURSUANT TO SE
SECURITIES EXC
AND SECTION 203
INVESTMENT AD
MAKING FINDIN
REMEDIAL SANC

2. On September 21, 2015, Marsh pled guilty to a criminal information in United States v. Galen Marsh, No. 15 Cr. 641 (KTD) (S.D.N.Y.) that charged him with one count of exceeding his authorized access to a computer and thereby obtaining information contained in a financial record of a financial institution, in violation of 18 U.S.C. § 1030(a)(2)(A). On December 22, 2015, a judgment in the criminal case was entered against Marsh. The court sentenced Marsh to 36 months' probation and ordered him to pay restitution in the amount of $600,000.

3. In connection with his plea, Respondent admitted that:

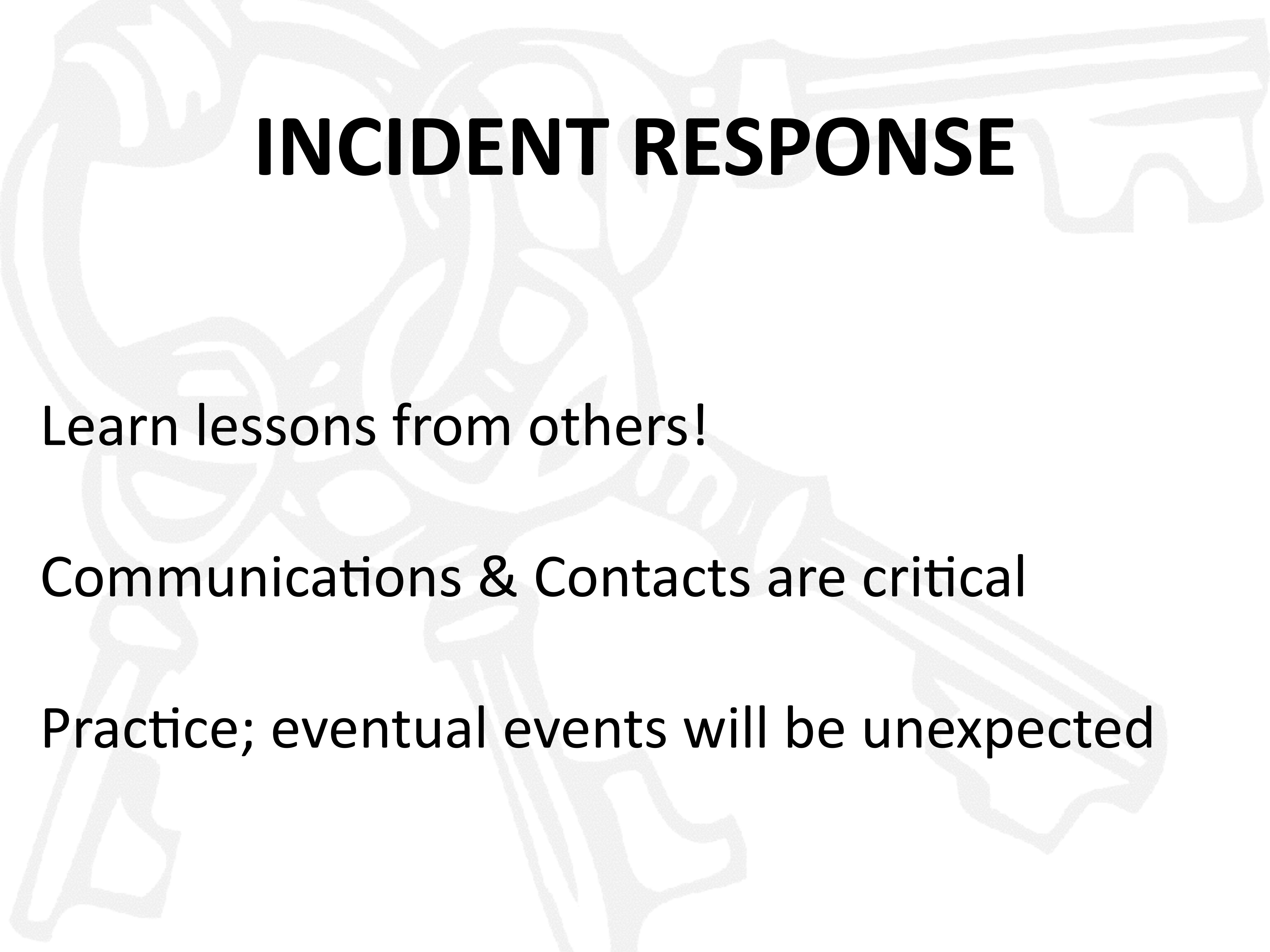
(a) beginning in approximately June 2011, he intentionally accessed MSSB's computer system, exceeding his authorized access, and thereby obtained confidential customer information; and

(b) this confidential customer information had a value of more than $5,000.

IV.

In view of the foregoing, the Commission deems it appropriate and in the public interest to impose the sanctions agreed to in Respondent's Offer.

https://www.sec.gov/litigation/admin/2016/34-78020.pdf



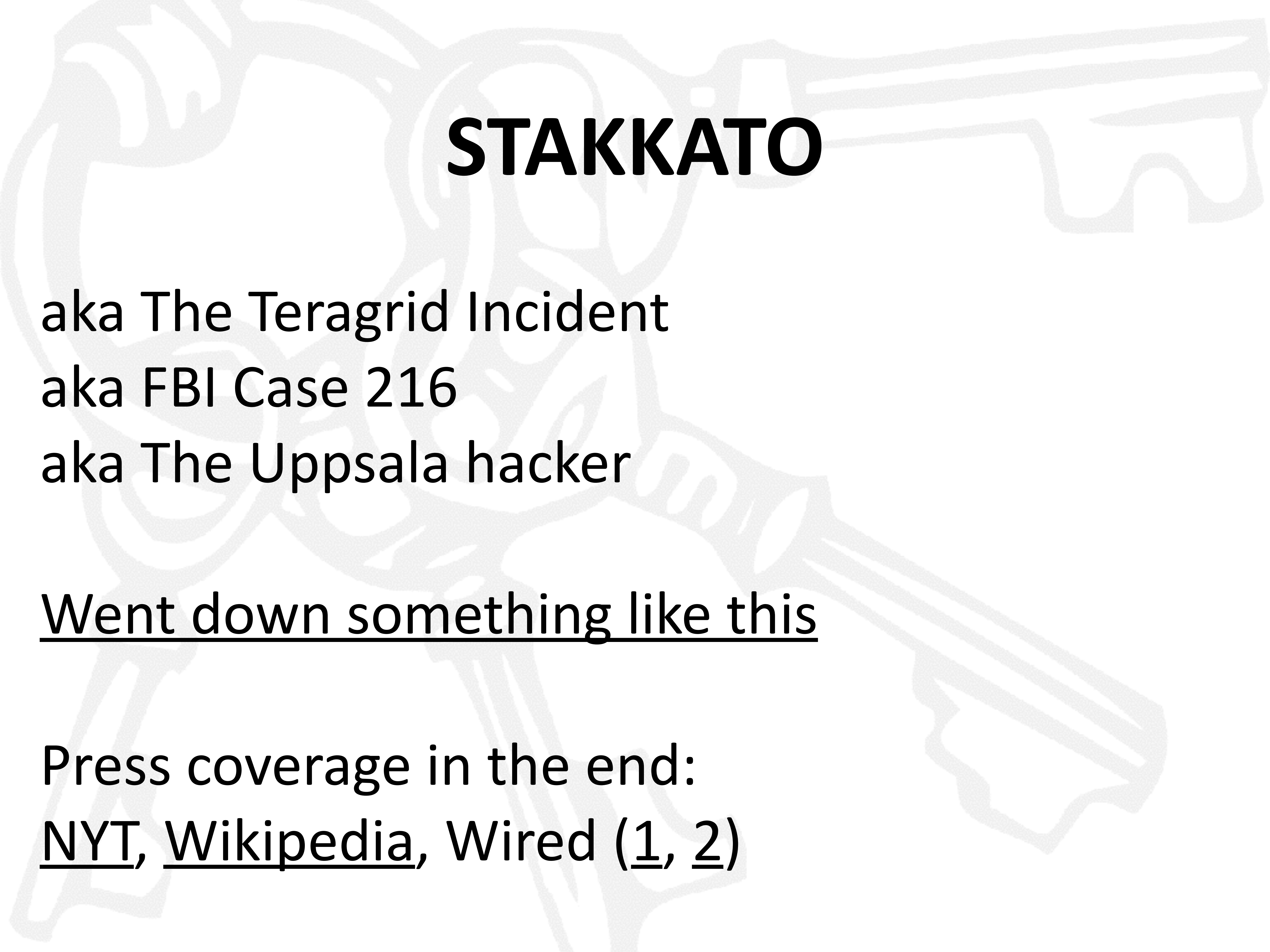
INCIDENT RESPONSE

Learn lessons from others!

Communications & Contacts are critical

Practice; eventual events will be unexpected

STAKKATO



aka The Teragrid Incident
aka FBI Case 216
aka The Uppsala hacker

Went down something like this

Press coverage in the end:
NYT, Wikipedia, Wired (1, 2)