A DAM SHAME

A DATA BREACH MOCK TRIAL EDUCATIONAL MATERIALS

THE PLAYERS

Judge: Claire Rosston | Holland & Hart LLP | ccrosston@hollandhart.com

Prosecution: Lee Holcomb | Lee Holcomb Consult | lee@leeholcombconsult.com

Defense: Brad Frazer | Hawley Troxell | bfrazer@hawleytroxell.com

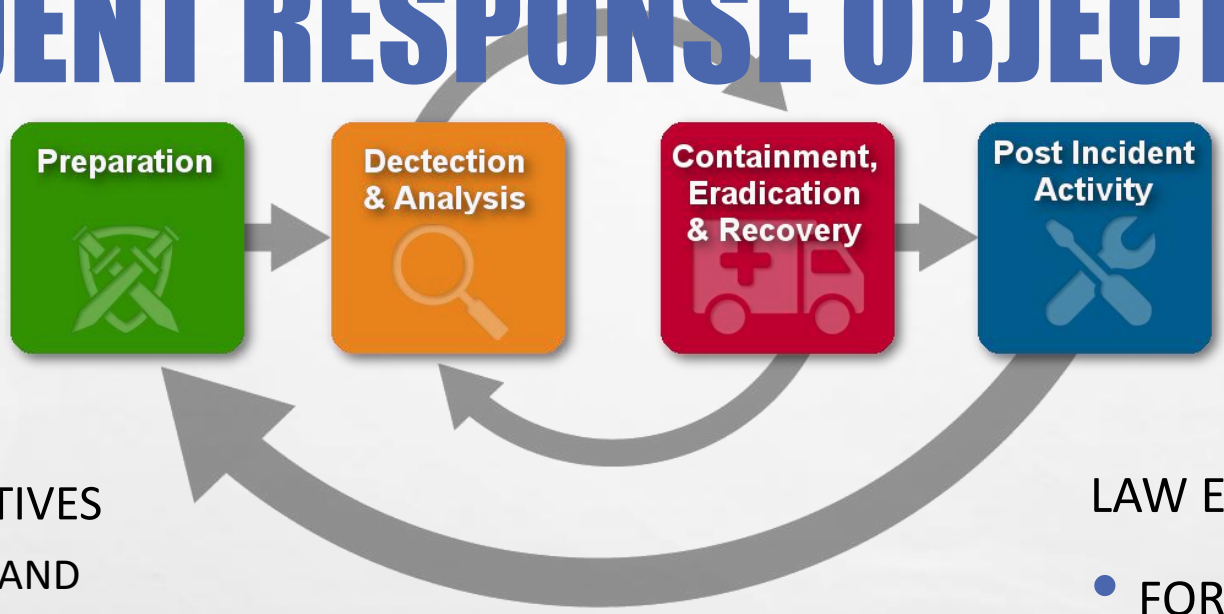
Fact Witness: Susan Buxton | DHR | susan.buxton@dhr.Idaho.gov

Fact Witness: Paul Wilch | Hawley Troxell | pwilch@hawleytroxell.com

Expert Witness: Clark Harshbarger | FBI | clark.harshbarger@ic.fbi.gov

Defendant: MacKenzie Brown | Microsoft | macbrown@Microsoft.com

INCIDENT RESPONSE OBJECTIVES



ORGANIZATIONAL OBJECTIVES

- CHAIN OF CUSTODY AND EVIDENCE PRESERVATION
- INCIDENT RESPONSE PLAN AND PROCEDURES
- REPORTING AND NOTIFICATIONS (REGULATORY IF APPLICABLE)
- AFTER ACTION REPORTING

LAW ENFORCEMENT OBJECTIVES

- FORENSICS, ANALYSIS, AND ATTRIBUTION
- TESTIMONY
- REPORTING

INCIDENT RESPONSE PLAN AND PRESERVATION OF EVIDENCE

An Incident Response Plan Should Contain:

- Definitions of a data security incident and a data security breach
- A plan for escalating data security incidents and breaches to the incident response team
  - Establish how employees can report cybersecurity events
  - Prominently promote reporting channels that are secure, confidential and available in multiple ways and accessible from different devices
  - Identify data security incidents that require immediate notification or escalation (i.e., what is considered "high-risk" and how high-risk situations will be directed and escalated)
- A list of all members of the organization's incident response team and their contact information, responsibilities and authorities
- The names and contact information for key external vendors who may assist the organization in responding to an incident
- Instructions for determining whether a breach occurred, containing the breach and preserving evidence
  - Include expectations regarding timing
- A process to inform your management, the board and others about the event
  - Include how often to report, what to report and the delivery format
- A plan for communicating externally with affected individuals, law enforcement, the media or business partners
- A requirement for post-incident analysis

Preservation of Evidence

- Circulate a litigation hold notice
- Remind custodians of their preservation obligation frequently
- Monitor custodian compliance
- Stop backup tape recycling as necessary
- Suspend enterprise-level document destruction as necessary
- Collect from departing employees

SAFEGUARDS

Administrative

- Policies and procedures, including security incident response procedures
- Auditing and monitoring compliance with policies and procedures
- Principle of least privilege: Access rights and administrative privileges only given when necessary
- Employee training
- Employee confidentiality agreements
- Service provider contractual obligations

Physical

- Controlling building access with a photo-identification/swipe card system and locked doors
- Maintaining equipment that contains or stores sensitive data to ensure its availability, functionality and integrity
- Minimizing the amount of sensitive data on desktops
- Protecting mobile, portable or easy to remove equipment, located inside or outside the facilities
- Secure disposal of data, such as shredding

Technical

- Antivirus software
- Authentication
- Data encryption
- De-identification of data
- Firewall
- Mobile device management
- Remote wipe capability
- Detailed logs (see NIST SP 800-92, Guide to Computer Security Log Management)

CYBER INSURANCE

Cyber insurance is a new product

- No ISO form like there are for general liability, auto, etc. so it's complicated
- Rapidly changing, negotiable and review of cyber policies is key
- Coverage can differ dramatically from one insurer to another for surprisingly different premiums

First-party coverage

- Covers forensics and notification costs and losses of policyholder from data breach
- Covers lost income and other harm to the policyholder's business resulting from breach
- Pre-approval or use of insurer's service providers often required

Third-party coverage

- Policyholder's liability to third parties arising from a data breach or cyber attack
- Some policies have "contractual liability" exclusions—preclude any recovery by the insured for costs related to indemnification of a third party—and others do not

KEY STATE LAWS: BREACH NOTIFICATION

Covers

All states and DC have a breach notification law

Which state's law applies depends on where the impacted person residence by the governor

Requirements

Trigger: Discovery or notification of breach

Deadline: Varies

Enforcement

Typically AG - Some states authorize civil suits by injured individuals

Liability

Injunction

Economic damages

Regulator costs

Fines

Federal breach notification

HIPAA breach notification rule

FCC privacy regulations

BEST PRACTICES WITH THIRD-PARTY SERVICE PROVIDERS

Have a written contract with the provider

- It's not just a best practice; it's the law:
  - Federal enforcement of § 5 of the Federal Trade Commission Act
  - Industry regulations in the financial and health care sectors
  - State law example: The California Data Protection Act requires all businesses with any California resident's personal information to contractually require an unaffiliated third party with access to such personal information to follow the business's same safeguards.

that contains contract terms that require:

- Proper physical, administrative and technical safeguards
  - Employee training
  - Written NDA with employees who receive customer's confidential information
- Compliance with applicable data security and privacy laws
- Indemnification
- Cyberinsurance

INSIDER THREAT CONSIDERATIONS

PROCESSES AND RESOURCES

- POLICIES, PLANS, SOP'S
- EMPLOYEE HANDBOOK
- NON-DISCLOSURE AGREEMENT
- ACCEPTABLE USE POLICY
- BACKGROUND CHECKS
- THIRD-PARTY RISK MANAGEMENT
- TERMINATION PROTOCOLS
- INCIDENT RESPONSE PLAN & PLAYBOOKS (RUNBOOK FOR CLASSIFIED INSIDER THREAT INCIDENT)
- BYOD POLICY (MOBILE DEVICE MANAGEMENT, INVENTORY)
- INSIDER THREAT PROGRAM (BEHAVIOR AND ACCOUNT ANOMALIES AND ALERTS)

BEST PRACTICES WITH DEPARTING EMPLOYEES

Obtain custody of the employee's company-supplied computers and mobile devices, as well as all external hard drives, thumb drives, backup discs, etc.

Obtain custody of company credit cards, security access cards, parking codes, etc.

Take an inventory of all of the files or projects on which the employee was working and make sure that all such materials have been returned. This is particularly important for employees who work remotely.

Require departing employees to sign a document indicating they have returned all corporate data assets.

During the exit interview ask the employee questions about future plans/employment to determine potential risk.

Give managers access to their employees' content archives.

Disable all accounts to which the employee has access, such as employee's Office 365 user account, access to the company network and the Active Directory user account or equivalent.

Change passwords for all applications, cloud-based storage, voicemail, etc.

Remove employee from all distribution lists.

Redirect employee communication (e.g., email) to an appropriate individual.

TAKEAWAYS

1. WRITTEN CYBERINCIDENT RESPONSE PLAN: KNOW WHOM TO CALL.
2. FORENSICALLY SECURE ALL EVIDENCE AND DATA OF THE HACK.
3. WRITTEN CYBERSECURITY POLICIES AND PROCEDURES.
4. CYBERLIABILITY INSURANCE OR SELF-INSURANCE.
5. LOGGING ALL NETWORK ACCESS.
6. PRINCIPLE OF LEAST PRIVILEGE: LIMIT ACCESS TO DATA TO “NEED TO KNOW”.
7. CONTRACTUAL OBLIGATIONS OF SERVICE PROVIDERS/CLOUD VENDORS.
8. EMPLOYEE TRAINING AND SIGNED POLICY MANUALS.
9. CERTIFICATIONS FOR SECURITY PERSONNEL.
10. EMPLOYEE EXIT PROCEDURES.
11. NOTIFICATION OBLIGATIONS TO INSURER TO INVOKE COVERAGE.
12. DATA BREACH REPORTING OBLIGATIONS FOR PII.