CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Integrating Security Incident Response and e-Discovery

Key Message: Responding to an e-discovery request involves many of the same steps and roles as responding to a security incident.

Executive Summary

E-discovery commences when electronic information is requested as potential evidence in legal proceedings. It turns out that a legal discovery request is much like the first notification of a security incident, in terms of the steps you need to take (triage, involving the right people, determining the extent of the event including what systems and information are involved, analysis including forensics, etc.).

In this podcast, David Matthews, the Deputy Chief Information Security Officer for the City of Seattle, discusses his team's approach for integrating computer security incident response with e-discovery.

PART 1: INFORMATION SECURITY FOR CITY GOVERNMENTS; DEFINING E-DISCOVERY

Unique Aspects of Managing Information Security for City Government

Typically, information security (IS) departments for city governments have fewer resources and limited control of their budgets. Most of what they need to accomplish is funded by other city divisions.

Obtaining executive buy-in is challenging, given a city mayor is elected every 4 years with priorities set by what matters most to citizens and constituents. In addition, mayors often have little to no appreciation of information security risks, and need to be educated.

Cities are organized as federated groups of municipalities and counties, and their governments have wide ranging and diverse lines of business such as utilities, public safety, justice, transportation, city council, etc. These tend to operate quite independently.

Cities are organized as federated groups of municipalities and counties, and their governments have wide ranging and diverse lines of business such as utilities, public safety, justice, transportation, city council, etc. These tend to operate quite independently.

Doing information security risk management on a city-wide basis and getting division leaders to work together can be quite challenging.

That said, one topic that does get the public’s interest is privacy – being able to ensure the public that their data is safe. Privacy helps information security officers get some traction with city government agencies.

E-Discovery

Discovery is part of any legal process, where the two opposing parties agree to discover and disclose evidence relevant to the case.

E-discovery is simply the discovery and disclosure of electronic information (ESI – Electronically Stored Information) in support of a legal proceeding.

E-discovery is becoming an increasingly important issue due to electronic evidence and electronic data being so ubiquitous. We all create electronic records every day with our computers and with the mobile devices that we use.

Often parties in a case will just settle rather than attempt to respond to e-discovery requests. Burying a defendant in these types of requests has become a weapon in the hands of plaintiffs' attorneys. There is often insufficient time and money to identify and gather all of the necessary information.

PART 2: BEING PREPARED FOR AN E-DISCOVERY REQUEST

Understanding Where Your Data Resides

Business leaders need to understand where their data is stored, including what devices or media it might be on and who owns the data.

For example, leaders typically don't consider door access key card information or digital output created by video surveillance cameras as data of potential interest for e-discovery. iPods and game consoles that are used in the work place can also contain relevant data.

Key questions to ask include:

- What are all of the places where data could live?
- How would you access it in response to an e-discovery request?
- How long would this take?
- How much would this cost?
- If you can locate all of the relevant data, how do you preserve it in a forensically sound manner so that you can prove its integrity in court?

Work with Records Management

Those responsible for records management know what the rules are in terms of what records need to be kept and for how long. When questioned in court, being able to show that you followed (and monitored) your records management procedures is key.

Work with Legal Counsel

Legal counsel needs to be able to answer all of the key questions above in court.

Legal counsel can assist in developing litigation hold policies and processes.

Executives tend to listen to their lawyers. With this in mind, legal counsel can be a great ally to help IS communicate information security risks.

Train Your Users

Records management and litigation hold policies are ineffective if users aren't adequately trained in terms of their roles and responsibilities.

Business leaders need to be able to demonstrate, in an audit, that users have been trained on all relevant policies and procedures, and that they follow them regularly.

If you have lost or destroyed key data that is called for during e-discovery but your actions were consistent with policy, this is generally an accepted defense.

New Actions for Information Security Staff

Security professionals tend not to consider information and records management, forensics investigation for legal purposes, and e-discovery – in effect, the entire legal side of how information is used and presented as part of a court proceeding.

Many of the same steps are involved here as when dealing with policy violations that could lead to employment issues that could then lead to lawsuits

---

PART 3: A COMMON PROCESS: INCIDENT MANAGEMENT AND E-DISCOVERY

Incident Management . . .

The City of Seattle created its incident response plan based on the U. S. government's ICS (Incident Command System) NIMS (National Incident Management System).

The genesis of ICS NIMS is fighting forest fires. It has evolved to become a standard system for any type of incident management and is broadly used by first responders (firefighters, police).

One of the advantages of using this system is having a common language when interacting with other organizations that are also using it.

The event management process includes:

- Triage: recognizing what the problem is, its scope, and its priority
- Gathering the right subject matter experts and stakeholders together
- Finding out more about the ongoing investigation
- Creating a plan of action, and executing it
- Evaluating what happened, and repeating the process
- Capturing lessons learned at the end

And What It Has in Common with E-Discovery

It turns out that responding to an e-discovery request involves many of these same steps with, perhaps, some different subject matter experts (for example, lawyers).

Recognizing and capitalizing on the commonalities between these two types of events are beneficial when resources are tight.

In David's experience, the city attorneys were very thankful to be given defined processes, procedures, and documentation to follow. Now the IS team is called upon every time there is a litigation action. The IT staff is also happy to have guidance in this area, as are the managers and users.

PART 4: KEY ROLES; STEPS FOR GETTING STARTED

Building the Event Response Team

There is not a standing team for responding to security events and e-discovery requests. A team is assembled depending on the event and the organizations that are affected.

IS serves as the coordinator for forensics investigations and litigation hold actions.

An Example Event

In this case, a local government office has a disagreement with a local sports franchise.

- The attorneys are contacted and they contact David.
- Triaging this event involves determining what data is most important and where it is likely to reside. If it involves email (which it typically does), who has it?
- Next determine if the email has been preserved, and if not, how to accomplish this.
- Direct email administrators to stop purging any emails for the involved parties.
- Gather the relevant subject matter experts including IT staff responsible for managing the email servers.
- Convene a meeting of the involved users and the attorneys to make sure everyone understands the scope of the issue by answering the following questions:
  - Where's the data?
  - Who owns the data?
  - Who is going to be responsible for gathering the data?
  - How is the data going to be preserved in a forensically sound manner?
  - Who is capable of doing this?
  - Plan, and evaluate the plan.

Those responsible for preserving data in a forensically sound manner must be trained to do it right or have someone knowledgeable monitor their every step. These actions need to be defensible in court with respect to data integrity and chain of evidence.

Forensics analysts are required to sign a litigation hold form attesting to the fact that they did preserve all of the data. IS ensures that the relevant data is held for as long as the case is active, sometimes years.

First Steps

The responsible business leader convenes a meeting with their attorneys, risk managers, records managers, IT and IS managers, and key staff.

IS plays a key role, as investigators or expert witnesses can challenge or defend an organization's evidence based on the strength of its information security program. This is due to the fact the information security controls help ensure data integrity and data preservation.

In this meeting, discuss all of the questions raised in this podcast. Discuss how your incident response plan can be integrated with the litigation hold process. Assign a champion to make this happen and provide them with sufficient staff and resources.

Keep in mind that for many organizations today, litigation is a daily event.

Resources

Incident Management Resources

U.S. National Incident Management System (NIMS)

U.S. Federal Emergency Management Agency Introduction to Incident Command System course

U.S. National Institute of Standards and Technology reports on incident response; specifically Special Publications 800-61, 800-53, and 800-86

CERT Computer Security Incident Response Team resources

e-Discovery Resources

Electronic Discovery Law web site; K&L Gates LLP

Discovery Resources web site

Withers, Kenneth. “Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure.” Northwestern Journal of Technology and Intellectual Property, Volume 4, Issue 2, Northwestern University, Spring 2006.

Ken Withers’ web site: Electronic Discovery Rules, Proposed Rules, Commentary, and Debate

LexisNexis Applied Discovery Online Law Library

Nixon Peabody Attorneys At Law. “Electronic Discovery: What You Need to Know and What It May Cost If You Don’t.” 27 October 2004.