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

Leveraging Security Policies and Procedures for Electronic Evidence Discovery

Key Message: Being able to effectively respond to e-discovery requests depends on well-defined, enacted policies, procedures, and processes.

Executive Summary

Most of today's law expects to have information in physical form when it is submitted as evidence. In contrast, digital information is volatile and created dynamically, which can make it hard to collect and can cause its reliability and credibility to be challenged in court.

In this podcast, John Christiansen, an attorney specializing in information security, compliance, and risk management, discusses how business leaders can be better prepared when called upon to submit digital information as evidence in legal proceedings. John is the founder of the Information Security, Compliance, and Risk Management Institute (ISC RMI).

PART 1: CHALLENGES IN PRESENTING DIGITAL INFORMATION AS EVIDENCE

Unique Characteristics of Digital Information

The law is used to dealing with information in physical form but is in catch-up mode in applying legal principles and standards to information in digital form.

The law looks backwards and deals with precedent. Information on paper doesn't degrade, can be preserved indefinitely, and changes to it are evident.

In contrast, digital information often does not exist in the way it is presented to a reader. It exists as bits and bytes that are processed by software applications. Information can be pulled from a number of sources to create and generate a printed version.

In other words, information is volatile and created dynamically – and it can be changed and corrupted inadvertently, or without authorization or the reader's knowledge.

And the Legal Issues this Raises

From a legal perspective, it is difficult to:

- make sure you have the right information
- make sure that you have all of the information

Information proliferates and copies can reside anywhere.

One example is patient health records. The physical file that a doctor consults today may be quite different from its digital equivalent as conditions and health status change. Changes can be accurate and intended, or they can be falsified.

Ramifications during Discovery

A knowledgeable attorney can bury the opposition in discovery requests if they are sophisticated and suspect that

information has changed or is not correct.

Such an attorney won't accept paper printouts. They will ask about log files, databases, and applications to test for the accuracy of the resulting information.

This type of questioning is used to either build confidence or question the validity of the presented information.

Getting Information that Matters into Court

Key questions that determine whether information is admissible in court include:

- Is the information sufficiently reliable? Standards are under development to determine this. Recent challenges include breathalyzer results and voting machine results.
- If I am the judge or a member of the jury, why should I believe the information? Is it credible? If an attorney can challenge the ways in which the information was produced, it may be rejected.

For a defendant to be found guilty in a criminal case, proof must be established beyond a reasonable doubt – a very high standard.

If an attorney can challenge the credibility of the proof/information (by challenging the way it was produced), the defendant may be found not guilty.

In civil cases, the rule is preponderance of the evidence – the proof results in slightly more weight or more belief in one direction. This rule is not as hard and fast. If an attorney can raise doubts, they win.

PART 2: BE PREPARED: POLICY AND PROCESS

Identifying and Preserving Relevant Evidence

When you are served with a summons or a complaint, your legal duty is to preserve all relevant evidence in your systems.

If you don't have policies and processes in place – and thus find yourself in reactive mode – fulfilling this legal duty is nearly impossible.

In this situation, your IT team is faced with a very difficult, burdensome forensic task to figure out who's responsible and what to preserve.

The Benefits of an Organized Response

Security incident response offers a useful model for dealing with a discovery request (where the information resides, how to find it, how to make sure it isn't changed, how to access the information, and how to use it).

If you have a solid policy in place that is being used (refer to Christiansen 08), people can address these aspects of a discovery request. While there is still a burden, your response will be more effective and efficient.

Having an organized response and set of established processes is a strong defense when challenged.

Having an organized response and set of established processes is a strong defense when challenged.

Judges typically recognize and accept good-faith efforts when you can't produce everything, need to narrow the discovery request, or need more time. Conversely, they can penalize you if they get the impression that you are not cooperating or managing your processes competently.

PART 3: INVOLVE KEY ROLES; PRACTICE MOST LIKELY SCENARIOS

Steps to Take

Put a strong policy in place that delineates responsibilities and accountabilities.

Business leaders generally know where most litigation will come from, given their history and market. Legal counsel will also know. So be prepared to respond to these types of requests. Conduct periodic table top exercises that address expected scenarios.

- For example, in healthcare, you are likely to be sued for medical malpractice – so practice cases of this type to make sure everyone knows their responsibilities.

Make sure your IT team knows who is responsible for gathering information and preserving evidence. Add the ability to identify and produce admissible evidence in digital form to the mission statement of your IT department.

The forensics expertise of your security staff is invaluable. They can investigate and then reliably state what happened with an application, a database, and the network.

Draw knowledge and best practices from other related disciplines: business continuity, disaster recovery, and incident response.

Make sure your general counsel understands the issues and knows what to do. They should be leading the charge.

Resources

[Christiansen 08] Christiansen, John. "Leveraging Security Policies and Procedures for Electronic Evidence Discovery." ISC RMI, Thursday September 11, 2008.

- This presentation and its supporting files contain sample policy language for information asset protection, authentication management, information system activity monitoring, and electronic evidence discovery response.

Christiansen's IT Law: Information Law Theory and Practice blog

The Sedona Conference

Information Security, Compliance, and Risk Management Institute

CERT Podcast: Integrating Security Incident Response and e-Discovery, November 11, 2008.