CSIA Data Integrity Summit
January 18, 2006
Panelist Notes

1. Corporate Government Panel:

Swindle: Who do you hold responsible?

Tomaszewski: Everyone. Trust must exits between a corporation and its consumers. The marketplace demands it.

Cohen: Data and security are one and the same. Risk management is generally the responsibility of the CEO, and the board. As a result, everyone at the highest level managing risk should be concerned with information management.

Winston: We need to focus on forward-looking remedies.

Geer: Security technology involves collecting the same numbers. People have historically been taught to take certain risks to increase their profit, but instead, we need to manage it, measure it, and improve it for profit.

Geer: Corporations generally only care about risk management if they one, have been recently embarrassed, or two, are in trouble with audits.

Tomaszewski: Confidence must be built, and trust must be maintained, at the CEO level.

Cohen: It is important not to wait until it is too late. You must create, persevere, and identify information.

Kuper: The threat is real, and many people end up asking: "Why did this happen to us?" Many times it happens when labor goes beyond borders.

Winston: We are currently dealing with widespread non-compliance in a target-rich environment. No one is taking this seriously, and thus, we need to get the message out through outreach, but unfortunately, this is the reality right now.

DC: We have a data rich future.

OS: Where exactly does the board fit?

CSIA Data Integrity Summit
January 18, 2006
Panelist Notes

Kuper: The CFO and board head positions are the hardest to fill because of the liability involved with the position.

Tomaszewski: Security and trust is good business.

Kuper: People tend to believe that security cost is a hindrance, when realistically, it can turn cost into profit. (Ex: E trade)

Cohen: Trust is a service to customers that can be used as a marketing tool.

Winston: BJ's Wholesale and DSW kept data they did not need.

Geer: About 2002, it became cheaper to keep everything.

Swindle: Getting the people to pay attention seems to be the hardest thing. Do you think they need more laws to make information security better?

Winston: It is a daunting task. The information is there, but there are gaps, and synthesis is needed for flexibility. It is important to encrypt, as well as establish, a reasonable standard as a safeguard. A process-oriented requirement is needed since it is not one size fits all.

Tomaszewski: Date integrity needs a process solution.

Cohen: Laws apply to specific information and industries. As a result, it is important to know who is accountable, the risk assessed, the policies affecting that risk, and what should be done if something does go wrong.. Thus, a common framework is necessary.

Kuper: We do not need anymore legislation because the use of data starts internally.

Cohen: SOX affects information management in terms of definition, the interpretation of broader information (certification must be driven through the organization), and document alteration / destruction.

Swindle: Is the sky falling?

Geer: Yes, in slow motion.

Winston: We must move towards a solution, or it will.

Kuper: Yes.

Tomaszewski: I think it is a blizzard of precautions, and ignorance will kill you.

Cohen: The sky does not need to fall, but there cannot be a gap between the way your information is managed, protected, and documented.

2. Legal Panel:

General Opening: It is important to remember that information security and identity theft is not simply a domestic issue.

McComas: In terms of record management and data integrity, there is intentional breaching, as well as unintentional breaching. Examples of unintentional breaching are version control, as well as archive sites, and tape management following system failure. How do they link to the document? Community standards and record management also create a gap between policy and practice. Legislation tends to set the standards.

Winer: In terms of international bridging, it is important to consider which legal regime data is under. (Ex: German law; Bavarian different than the rest, etc. ) Also, are the standards in the beginning able to be applied across the board? It is extremely important to encourage compliance with international standards as well. You do not want a gap between professed obligations.

Sabett: The role of an attorney with data integrity involves risk management, and considering what is / is not reasonable. There generally is no clearly defined way for a company to fulfill its financial obligations, and many issues are no longer simply black

and white. As a result, the threat to your vulnerability is your risk. It is important to evaluate the steps you have taken to manage this threat, and thus, your overall vulnerability.

Winer: It is not about reasonableness, but the outcomes. I believe that there is a close gap between professing, and doing.

Paul: There is an "Authenticity Crisis." Information records are artifacts, and need to be tested as such. There has been a revolution, and now records are components in complex information systems. Crisis exists because our current system is based upon an old paradigm, and we are now using information ecosystems. Is it important to always test the authenticity of this information, when, for example, it is edited? Just because you cannot always prove that it is authentic does not mean it isn't.

Tritak: Why not just make copies?

Palmieri: We can mainly learn and get information from real-life cases and experiences. After all, most electronic evidence is found in e-mails. It is also our duty to preserve litigation holds first, while also suspending routine destruction practices. Counsel is needed that is knowledge about active e-mails. Back-up tapes need to be preserved to avoid a lack when requested. Situations involving negligence need to be avoided: (Ex: "I received the e-mail, but I receive hundreds of them a day. How was I supposed to know it was there?")

McComas: General Counsel will no longer look the other way.

Winer: We need to also focus upon government information and retention policies.

Question (afterwards): What if you do now know what you are holding and that there is a breach?

Answer: You are still held accountable for that information.

3. The CSO / CIO / CISO Panel:

Nearon: Integrity is typically thought of as a personal issue. It can refer to someone or something being honest and trustworthy, or to information, like structural integrity.

The closest definition to informational integrity with accounting is representational effectiveness; meaning: Who created it? When was it created? Is there a high probability that it has not been changed since its creation? All these questions are necessary to know to maintain representational effectiveness.

Nearon: To do this, do you need general practices, or intentional planning and action?

Schmidt: A consistent plan is needed for integrity, and the use of the information down the road.

Doyle: Data's context is also important. If the context changes, how can there be much confidence in its unaltered state?

Nearon: What role does security and IT play?

Scharf: What it comes down to is: What data we do / don't focus on? To answer such a question, a joint effort between groups is necessary, and the data should be based on a classification model.

Nearon: Where is the assertion regarding integrity made? Who, when, etc? And if you assert it, is it accurate? It's like a chain of custody.

Nearon: What is the role of the digital signature, etc?

CSIA Data Integrity Summit
January 18, 2006
Panelist Notes

Guida: It ensures that if someone cannot verify it at a later date, something is most likely wrong. It tells who actually signed it. Engineers and lawyers need to know about one another.

Sorebo: They show signs of weakness that could also show reductions in trust.

Doyle: Record keeping shows data in a moment in time. It is different to measure / test change. How do good insiders prove they did not misuse their right to dispose? The evidence should be in the data, and empirically tested. Data integrity is from a point in time when time can be proven.

Schmidt: Consider the life cycle of data and signatures.

Scharf: Some technologies, like encryption, can do more harm than good.

Guida: What technologies do, versus what products can do? For example, the historical significance checking tool. Technology supports it, but not the tools. It is product limitation, and not technology.

Question (afterwards): Is it not important if it is misused?

Answer: It depends on whether it is internal, or external use.

Question: Concerning identity provisioning with multiple different organizations…who can attest to the integrity of the data?

Sorebo: There are certain assumptions existing about e-mails and information access. The process is in place saying you are who you say you are.

Guida: Trusting different security infrastructures must be correct.

Scharf: There is also a linkage between systems so accounts end..

Doyle: There is a large difference between identity, and integrity.

Schmidt: Conclusion: A fundamental dialogue is needed.