Aslam, Taimur, Ivan Krsul, and Eugene H. Spafford. "Use of a taxonomy of security faults." (1996).

Look at:

C. M. Curtin and L. T. Ayres, "Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry," I/S: A Journal of Law and Policy for the Information Society, vol. 4, no. 3, Winter 2008-09.

Standardizing Breach Incident Reporting: Introduction of a Key for Hierarchical Classification --- This is an archaic research paper and rather stupid.

Ayres, Lee T., C. Matthew Curtin, and Thomas A. Ng. "Standardizing Breach Incident Reporting: Introduction of a Key for Hierarchical Classification."*Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on*. IEEE, 2010.

Garrison, Chlotia Posey, and Matoteng Ncube. "A longitudinal analysis of data breaches." *Information Management & Computer Security* 19.4 (2011): 216-230.

-- they have a crude hierarchy, but apply several statistical tests, worth reading carefully

From that:

Based on the analysis, the breaches were divided into five categories: stolen, hacker, insider, exposed and missing. The stolen category includes stolen hardware such as desktop computer, laptop, server, flash drive, and hard drive. The hacker category covers unauthorized remote computer break-ins. Insider involves misuse of access/authority of computer usage by an employee or former employee. The exposed category involves unprotected data that may be publically accessible and includes records exposed in e-mail, regular mail, online and through disposal. The missing category includes missing disks, files, hard drives, flash drives, tapes, laptops, computers and servers. The breached data consisted of personal information, such as social security number, about current, former, and potential employees, customers, parents, dependents, guardians, and other individuals that used the services of the affected institution.

The data are analyzed using six institution types: business, education, federal/military, financial, local/state government, and medical. The Open Security Foundation's DataLossDB uses four categories: business, education, government, and medical ([15] Open Security Foundation, 2010-2011). The ITRC uses five categories: banking/credit/financial, business, education, government/military, and medical/healthcare ([11] ITRC, 2010-2012). This study separates the federal government from state and local government because of its potential for a breach to affect a broader population than state and local government.

Kannan, Karthik, Jackie Rees, and Sanjay Sridhar. "Market reactions to information security breach announcements: An empirical analysis."*International Journal of Electronic Commerce* 12.1 (2007): 69-91.

----- meh, dated, from 2007

Adebayo, Adewale O. "A Foundation for Breach Data Analysis." *Journal of Information Engineering and Applications* 2.4 (2012): 17-23.

This is worth while to read, has numerous sources and opinions (no real work here though).

Adebayo, Adewale O., Yinka A. Adekunle, and Olawale J. Omotosho. "System and Data Capture Framework Insights into Breach Data toward Improved Feedback." *Innovative Systems Design and Engineering* 4.3 (2013): 20-31.

Adebayo, Adewale O., Olawale J. Omotosho, and Yinka A. Adekunle. "Statistical Insight into Breach Data toward Improved Countermeasures."*Information and Knowledge Management*. Vol. 2. No. 8. 2012.

(related to above, same authors)

Breier, Jakub, and Ladislav Hudec. "New approach in information system security evaluation." *Satellite Telecommunications (ESTEL), 2012 IEEE First AESS European Conference on*. IEEE, 2012.

* This actually uses VERIS to inform an AHP process.

Durowoju, O., and Hing Kai Chan. "The role of integration in information security breach incidents." *Proceedings of the Seventeenth International Working Seminar on Production Economics, Innsbruck, Austria, 20-24 February*. Springer, 2012.

Great quote:

<https://twitter.com/ATJCagan/status/355469205178556416/photo/1>

“I was exhilarated by the idea that you can understand what you see around you in terms of things that cannot be observed directly, but which explain what you see”

Measure what would explain what we see,

“We cannot measure directly what we see, but we can measure the parts of the whole that help explain what we see.”

In other words, if you can’t learn by directly measuring, you can measure based on assumptions: “if the value we care about is <quantity> then we should also see, x, y and z. Do we?”