AGENDA
A Financial Times Service

Tech That Defends Directors

By Tony Chapelle March 23, 2017

Whether seriously or in jest, we've all heard, "There's probably an app for that." Well, technology experts say board members should know about — and encourage senior managers to deploy — new apps and computer programs that could help fend off lawsuits that charge directors with negligence or poor oversight.

This software includes systems for e-discovery, internal audit management, and round-the-clock or so-called pervasive governance, risk management and compliance (GRC) monitoring. In many cases, these programs sift through tons of a company's e-mails, documents, and employee and customer records to find where and when the enterprise is afoul of law or regulation.

Protecting the Board

Several laws, such as Dodd-Frank, currently require boards to prove they have systems in place to mitigate operational risks and human mischief. If some matter still goes awry and a plaintiff files a suit, the board's risk management oversight will be challenged. Nicola Sharpe, a law professor at the University of Illinois at Urbana-Champaign, says a board would find it difficult to argue that it had a governing system that effectively identified risks unless that system could aggregate the entire enterprise's data along with recognizing the laws in the jurisdictions in which it does business and in which its third-party suppliers operate.

These new software advances allow for just that. "It's going to be harder and harder for [boards] to say we didn't know," says Sharpe.

The stakes are high, and the challenges companies face continue to evolve.

For instance, in today's digitally connected world, thousands of American multinational corporations digitally transfer data about Europeans into the United States. Yet in January, President Donald Trump signed an executive order that directed federal agencies to disregard current privacy laws when it comes to tracking foreigners who enter the U.S. That might have meant Europeans' personal information would be bulk surveilled when it comes into the country.

Tech That Can Keep Directors Out of Hot Water

Product	Type of Tech Tool	Maker	What It Can Do
Archer	Internal auditing	RSA Security	Searches company's regulatory, compliance and IT data for conflicts in jurisdictions where company does business.
Intelligent Migration	Data migration/ early data assessment	Nuix Pty. Ltd. (Australia)	Transfers millions of e-mails from company archives to the cloud. Identifies and disposes of unneeded data.
Product Compliance Management	Continuous monitoring	MetricStream	Updates lists of suppliers, manufacturing sites and restricted substances and screens products to comply with safety regulations.
Radiance	e-discovery	FTI Consulting	Sifts electronically stored information such as email, office documents and other unstructured data that may be required in civil suits.
Ringtail	e-discovery	FTI Consulting	Helps corporate lawyers defend better by finding all relevant documents for regulators or courts.
Risk Center	Risk & compliance	Dow Jones & Co.	Open-source online research on third-party vendors and business partners.
Risk Reports	Risk & compliance	Dow Jones & Co.	Large-scale background screening for foreign officials' ties, FCPA compliance and anti-money-laundering concerns.
Slack; Trello	Continuous monitoring	Slack Technologies (Canada); Trello Inc.	Collaborative (file-sharing) software can spot suspicious transactions and notify appropriate persons.

Source: Dow Jones + Co., FTI Consulting, Nuix Pty. Ltd., MetricStream, RSA Security, Slack Technologies and Trello Inc.

Afterwards, the European Union and the Trump administration hammered out a hurried agreement to ensure that the U.S. would abide by a previous "Privacy Shield" law that would keep European citizens' data private under EU global regulations. Under one of those rules, called the General Data Protection Regulation, if information about an individual European's private, professional or public life — even a computer IP address — is used outside the EU without permission, a company could be fined 4% to 5% of its global annual revenue.

"That's another board level concern," says **Jake Frazier**, senior managing director of the information governance and compliance services team at **FTI Consulting**. FTI specializes in litigation and forensic consulting, corporate finance and technology advising.

Frazier says that boards are comprehending the importance of information governance, that is, the ability to manage the millions of documents an enterprise churns out. "The reports show us where all of the data is, especially the risky data. File shares or shared drives, such as companies' B-drives or S-drives, are perfect examples. Sometimes you find compensation statements in them that show salaries. Shared files are the easiest place to get into a network. No one pays attention or goes through and sees what their risk is. But boards are now starting to do that."

Frazier's favorite case study is about how FTI came up with a plan to protect a bank client. The bank had file shares with personally identifiable data stored in Europe, Asia and North America. To protect European citizen-customers outside the EU, FTI employed technology for the bank to scan

and identify enterprise data but which prevented its Europe-based servers from leaking. Frazier said he used two pieces of tech: IBM's StoredIQ and FTI's Ringtail.

StoredIQ is a tool that uses what's called parent-child architecture to go collect data from a company's file shares, classify it by, for instance, identifying who created the data, and then index it.

"We ran single classifications from the parent screen that sent commands to the children servers in local jurisdictions asking if they had, for example, any personal health information. We may not want to bring it back so as not to violate their privacy laws." The multiple child servers all worked in parallel. Each one processed five to 10 terabytes of data to create one large index.

But to get the next level of detail, Frazier says, his analysts used an FTI product called Ringtail. This e-discovery platform processes and culls data such as trade secrets and gets smarter with the more feedback it gets. Using machine learning, Ringtail makes intuitive adjustments and uses algorithms for concept clustering and predictive coding to determine which information and shared files on the bank's servers are required to be under lock and key in a protected repository — what Frazier calls the corporate crown jewels — and which could be redacted.

"Sometimes there's no systematic disposal of information. Companies just hoard data forever," says Frazier. "If it isn't on 'info hold,' the best way to exceed privacy protection is to delete."

The entire process at the bank took six months. FTI says the work ultimately eliminated a large number of regulatory and possible legal risks for the company.

Deletion as Defense

One tech board member who started his career in mechanical engineering strongly advises boards to take advantage of programs that can delete sensitive material with discretion. John E. Major, a former chief technology officer at Motorola (now Motorola Solutions) and a director at Lennox International, Littlefuse and Orbcomm, advocates virtual board books.