AGENDA

A Financial Times Service

Opinion

Apply Y2K Urgency to Managing and Protecting Enterprise Information

May 23, 2016

When businesses faced the challenge of Y2K as the calendar approached 2000, there was a palpable sense of urgency across the globe. Managing corporate information, communications and systems potentially exposed by a computer program that interpreted dates inclusively between 1900 and 1999 instead of between 2000 and 2099 was a top business priority. Becoming Y2K compliant was critical.

There has since been an explosion in the growth of data and digital information, as well as myriad new regulatory, compliance, legal and cyber-related risks. But few organizations today demonstrate the same united resolve or are prepared with the right leaders and strategies in place to meet these risks head-on.

Mark Kindy is a managing director with **Alvarez & Marsal** Global Forensic and Dispute Services in New York, where he is the co-lead of their forensic technology services practice and a member of the global executive committee.

Reinvigorating a Y2K mind-set to help prevent future compliance, legal and cyber threats requires understanding and protecting an organization's enterprise information. Appointing a chief data officer (CDO) or chief information governance officer (CIGO) with boardroom clout is an important step, as is conducting information mapping across the entire enterprise.

Explosion of Data and Cyber Risks

Y2K may be behind us, but the digital threats to corporate information are more significant than ever as organizations contend with the evolving landscape of data, information, cyber security, cloud computing and digital channels. The explosion of data is only increasing; by 2020, 1.7 megabytes of new information will be formed every second by every person.

Exponential data creation is snowballing the risks of liability, exposure, job loss, financial stress and potential irreparable reputational damage for corporations. These threats put the overall security and safety of society at risk. In a recent Ponemon Institute study, out of 350 companies surveyed in 11 countries, the average cost of a data breach reached $3.79 million, a 23% increase since 2013.

As a result of the increased liability costs, more companies are purchasing cyber insurance. According to Marsh, there has been a 27% increase in cyber-insurance purchases by its U.S. clients. These companies also bought higher limits — $16.9 million of coverage on average, an increase from $14.7 million in 2014.

Invite a CDO or CIGO to the Boardroom

With the proliferating risks and costs associated with the management of data, the pressure is on board members and company executives to understand the full range of regulatory, compliance, legal and cyber risks, and to take a proactive stance to prevent future risks. Chief information officers and other executives can even be brought to court and held legally accountable as part of the e-discovery process. The SEC is also developing enforcement actions against companies relating to cyber attacks and the threats these attacks pose to markets, companies and investors.

For companies ready to improve the poor housekeeping of their data and prepare for future threats, a CDO/CIGO is a critical and indispensable role. Not only do companies need to add this role to their C-suite, but a CDO/CIGO needs to have a real seat in the boardroom with the authority to take action on behalf of the company to protect its data.

Secure Data through Information Mapping

With a CDO/CIGO on board, companies should perform a comprehensive information audit and mapping of enterprise-wide information to detect vulnerabilities. This means turning over every rock to identify all applications, information sources and data to determine what is valuable, which systems talk to each other, how data is currently protected and where the data resides.

The CDO/CIGO can then implement real improvements to the organization’s enterprise information program, including the proper categorization, prioritization, protection and destruction of data.

Acute awareness, along with the ability to anticipate cyber threats and protect corporate data, is required even more today than when Y2K ushered in the 21st century. Evoking the urgency of Y2K by securing a CDO/CIGO with the authority to map your organization’s data will ensure your protection against today’s — and tomorrow’s — threats.