PRESENTED AT

Conference The University of Texas School of Law
45th Annual Corporate Counsel Institute

May 4-5, 2023
Houston, TX

The Doomsday / Not Doomsday Update:

Data Privacy, Cybersecurity, and Data Protection Risks in 2023

Kathryne (Kate) M. Morris

Author Contact Information:
Kathryne (Kate) M. Morris
Hosch & Morris, PLLC
8117 Preston Road, Suite 300
Dallas, TX 75225
kate@hoschmorris.com
214.306.8980

Table of Contents

The Doomsday / Not Doomsday Update:
Data Privacy, Cybersecurity, and Data Protection Risks in 2023

Summary: *Not every data-related issue presents an existential risk. Here, we'll focus on the most significant risks, specifically, the data privacy, cybersecurity, and data protection issues that should matter to in-house counsel and motivate stakeholders within their organizations. In addition, we'll examine the latest legal developments, including case law and regulatory actions, making a case for enhanced executive oversight, recognizing governance and whistle-blower risks associated with chief security officers, and addressing the privacy and data security problems presented by organizational siloes.*

Have you ever wondered why data privacy, cybersecurity, and broader data protection issues often are metaphorically accompanied by an ominous soundtrack, like a funeral dirge with a deep drumbeat sounding at each new data breach, regulatory action, and new regulation? After all, not every compliance issue presents an existential risk, and thankfully, orange has yet to become the new black for lawyers who must deal with these often-esoteric issues (though orange may soon suit Uber's criminally-convicted former Chief Security Officer (CSO) – more on that later...).

This paper will focus on the risks that should matter to in-house counsel in 2023 – How to recognize critical cybersecurity issues, make a case for enhanced executive oversight, identify governance and whistle-blower risks associated with CSOs, and address the privacy and data security problems presented by organizational siloes. In the process, it will arm the reader with the latest information on data breaches, regulatory actions, and new rules, which should help as you advocate within your organization and perhaps provide the perfect motivation for reluctant stakeholders to acculturate themselves to latest privacy, cybersecurity, and data protection issues (all set to a blaring doomsday soundtrack or clock-countdown, as it were, to ensure you have everyone's attention).

I. Spotlight on Cybersecurity

Let's start by highlighting the most critical cybersecurity issue and gravest risk – Your organization being taken down by a cyberattack.

This isn't a hypothetical risk. Cyberattacks have disrupted businesses, research institutions, pipelines, nuclear reactors, dams, water-treatment plants, and more. *See* Zetter, K., *Countdown to Zero Day: StuxNet and the Launch of the World's First Digital Weapon* (2014); Greenberg, A., *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (2019); and Perlroth, N., *This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race* (2021). The shutdown of the Colonial Pipeline and resulting fuel shortages serves as a recent example of the crippling effect of cyberattacks. *See* Segal, E, 1 Year Later: Actions Taken, Lessons Learned Since The Colonial Pipeline Cyberattack, Forbes, https://www.forbes.com/sites/edwardsegal/2022/05/07/1-year-later-actions-taken-lessons-learned-since-the-colonial-pipeline-cyberattack/ [http://bit.ly/41X7ZC3]

When a cyber incident compromises an organization's operations, the organization's ability to conduct its business and serve its customers is also compromised, leading to financial losses and reputational damage. Critical systems and data risk being stolen, modified, or deleted in such cases. Unrecovered data potentially causes even more widespread disruption to operations. The attack might also affect employees' ability to access company resources, decreasing productivity. The organization must also dedicate significant resources to addressing the attack, including hiring experts to identify the vulnerabilities, deploying patches, and implementing new security measures. The process of recovering from such an attack is time-consuming and expensive. The legal fall-out is substantial (and that understates it). Cybersecurity threats are among the most significant and growing issues confronting companies and our country.

A. Operational Technology (OT) vs. Information Technology (IT) Cybersecurity

When it comes to cybersecurity, many organizations make the mistake of focusing on Information Technology (IT) over Operational Technology (OT). While IT and OT are two different domains of technology with unique issues, increasingly, they have overlapping cybersecurity concerns, which should be addressed systematically by stakeholders, including the legal department and executives within the organization, such as the chief technology officer (CTO), the chief information officer, (CIO), and the chief security officer (CSO).

It is essential to recognize that over the years, nation-states and other malicious actors have increasingly targeted OT systems and critical infrastructure, mainly because those systems have become more connected to IT networks and the internet. *See National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/ [http://bit.ly/3kUSE4o]. Efforts to comprehensively address cybersecurity should include considering IT and OT systems, prioritizing those systems that support critical business operations, and appreciating the differences and overlaps between those systems.

OT cybersecurity focuses on ensuring the availability and integrity of critical equipment and processes, relying on solutions like security information and event management (SIEM), which provides real-time analysis of applications and network activity, and next-generation firewalls (NGFWs), which filter traffic coming into and out of the network. *See IT vs. OT*, Fortinet, https://www.fortinet.com/resources/cyberglossary/it-vs-ot-cybersecurity [http://bit.ly/41RJXIC]. OT refers to the use of hardware and software systems that interact with physical processes in the real world, such as manufacturing (*i.e.*, automated warehouses), energy production (*i.e.*, turbines and pipelines), and transportation (*i.e.*, railroads and planes). OT encompasses the cyber-physical systems (CPS) that monitor and control industrial processes, equipment, and machinery, with the goal of optimizing efficiency, safety, and reliability. *See id*. Examples of OT systems include industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs). *See id*.

IT cybersecurity focuses more on confidentiality by helping organizations store and transmit data securely. *See id*. IT refers to the use of hardware, software, and networking technologies to manage and process digital data and information. IT systems are commonly used in office settings, such as in data centers, computer networks, and software applications. IT systems are designed to store, process, and communicate information with the goal of increasing productivity, efficiency, and communication. *See id*. Examples of IT systems include enterprise resource planning (ERP) software, customer relationship management (CRM) software, and computer networks. *See id*.

In your organization, consider who "owns" security for OT and IT. Are the necessary stakeholders, including the legal department, regularly coordinating? Metaphorically speaking, do the executives have oversight over what the left and right hands are doing?

B. Regulatory Developments

1. Executive Action, Memoranda, and a newly released National Cybersecurity Strategy

The Biden-Harris Administration has been active in its cybersecurity efforts, releasing an executive order and several memoranda focused on Federal Information Systems:

- National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity) (May 12, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ [http://bit.ly/3YACmeE];

- National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems) (July 28, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-

Title search: The Doomsday/Not Doomsday Update: Data Privacy, Cybersecurity and Data Protection Risks in 2023