COSMOS
Navigate the Compliance Universe

The Complete Compliance and Ethics Manual 2023
Security Incident and Data Breach Response

By Doug Pollack, MBA, CIPP/US[1]

Overview

Experts agree that security incidents and data breaches have become an everyday cost of doing business. The Verizon 2017 Data Breach Investigations Report analyzes over 40,000 security incidents and more than 1,900 data breaches across 20 industries.[2] Massive breaches, such as Sony,[3] Anthem,[4] and Target[5] have made headlines for months. However, smaller organizations are also at risk. An 18-bed county hospital in Illinois made news when hackers threatened to make 12,000-plus patient records public unless the hospital paid a ransom.[6] No company, regardless of size or industry sector, is immune to privacy/security incidents and data breach.

Data breaches are costly to both companies and their customers. According to the IBM-sponsored 2016 Cost of Data Breach Study: Global Analysis by Ponemon Institute, the average total cost of a data breach for participating companies grew 29 percent in the past two years to $4.0 million.[7] The price of a breach, of course, extends beyond immediate response costs to business disruption, regulatory fines, lawsuits, customer churn, and brand damage, the effects of which can be felt for years to come. For customers whose data was compromised due to a breach, identity theft in all its forms is also a concern. The Ponemon/Medical Identity Fraud Alliance study, 2014 Fifth Annual Study on Medical Identity Theft, found that medical identity theft nearly doubled in five years, from 1.4 million adult victims to more than 2.3 million in 2014.[8]

Much of the media focuses on the security aspects of incidents and data breach. Yet privacy and compliance officers have just as critical a role in mitigating the potential harms from incidents and data breaches as their information security counterparts. Companies must understand and abide by complex, even conflicting regulations when responding to incidents and managing breach notification. The failure to do so increases the likelihood of greater regulatory scrutiny and punishment, as well as for more and worse harm to customers. This article provides compliance officers with an overview of the cyber risk environment, as well as organizational barriers to overcoming these risks; a discussion of the regulatory landscape and how it applies to incident response and breach notification; and, finally, best practices and a 12-step checklist for responding to incidents and managing data breach notification in a caring and compliant manner.

The Cyber Risk Environment

Cyber threats to regulated data are wide ranging, and include, but are not limited to:

- Employee negligence or carelessness
- Lost or stolen devices
- System or application glitches
- Third parties
- Individual hackers

- Organized crime rings
- Adverse nation-states.

These threats, which put data at risk for unauthorized exposure and possible data breach, are exponentially greater in a world where data is no longer contained within the security perimeter of a single organization. Scott Johnson, who leads Unisys's Stealth security solution and product strategy, cites three reasons for this so-called "vanishing perimeter."[9]

1. The exploding volume of easily accessible data. Johnson cites an IDC estimate, that in 2015 "there will be approximately 2 exabytes of enterprise level unstructured data available.... One exabyte of storage could contain 50,000 years' worth of DVD-quality video...."
2. The number of "access types," including the 7 billion mobile devices. Cloud computing, too, alters the way data must be secured.
3. The "increased sophistication of the attackers and the attack types."

Finally, companies are struggling with the growing rate and complexity of cyber attacks. According to John Riggi, section chief of the FBI's Cyber Outreach Section, Cyber Division, noted that cyber threats by both nation states and organized crime are growing, most typically from Eastern Europe, Russia, China, and Iran.[10] "There are two kinds of big companies in the United States," James Comey, former director of the FBI, has said. "There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."[11]

The motivation behind these attacks is not always clear. Certainly there is a monetary incentive. Forged identities are one of many commodities for sale on the dark web.[12] Medical records, in particular, are attractive to criminals—they can access a patient's name, DOB, social security and insurance numbers, and even financial information all in one place. "Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70," said Jim Trainor, the FBI's former deputy assistant director.[13] In fact, criminal attacks on medical records are up 125 percent since 2010 and are the new leading cause of data breach in healthcare, the Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data by Ponemon Institute shows.[14]

Other reasons for cyber attacks are more obscure. The most recent Sony breach, for instance, is still believed by many to have been a result of a government sponsored cyberattack by North Korea to stop release of the film "The Interview," but the damage[15] went far beyond hurting sales from a single film. In fact, the breach became a model of many of the new risks surrounding cyberattacks and the resulting data breaches: disruption of business operations; intellectual property theft; public embarrassment; and damaged relationships with business partners, clients, and employees. With the Anthem breach, there was speculation that organized cyber-criminals may hold medical records for ransom, demanding payment for not releasing the information online or to other criminal groups.