Safety In Numbers: Cybersecurity 101 for the IRO

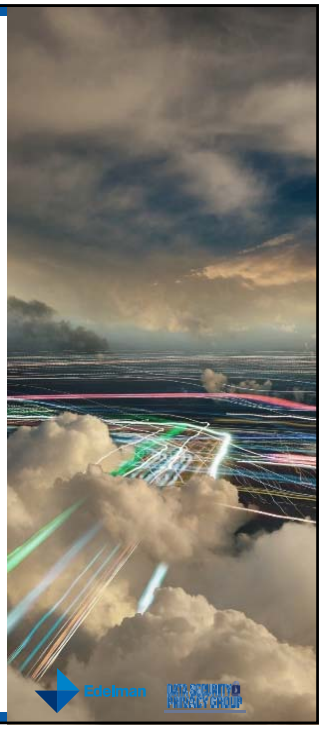
Andrew Liuzzi
U.S. Crisis Lead, Data Security & Privacy Group

Edelman

DATA SECURITY & PRIVACY GROUP

OPERATING REALITIES

- The speed of risk has become 140 characters or less.
- The traditional concepts of containment are no longer possible.
- Facts are negotiable.
- There are no safe havens from digitally empowered agendas and social exposure.
- **Data security and privacy has moved from the backroom to the board room.**



"AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE."

The average data breach in the United States costs an organization more than $6.5 million in investigations, customer notification, lost business and reputation management.

Organizations with an "incident response plan" at the time of their breaches saw an average cost that was $42 per record less than the national average per compromised record.

Edelman DATA SECURITY & PRIVACY GROUP 3

A NEW DRIVER OF REPUTATION & BUSINESS SUCCESS

EDELMAN'S SECURITY STUDY SHOWS:

- A gap between consumer expectations and what businesses are actually delivering
- A relationship between effective data protection and business success
- That data security and privacy considerations do impact purchasing decisions

Americans proved most loyal to the companies they do business with, yet ONE in TWO say they are likely to change brands after a data breach

71% Of global consumers would SWITCH PROVIDERS after a company they rarely used suffered a data breach

ACTIONS TAKEN FOLLING DATA BREACH EVENTS

39% Of global consumers TOLD A FRIEND about their experience

29% Of global consumers POSTED ONLINE about their experience

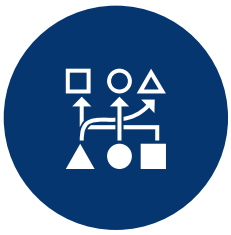
Edelman DATA SECURITY & PRIVACY GROUP 6

FAIL TO PLAN…PLAN TO FAIL

NO organization is immune to a cyber attack or data breach

NO amount of technology can account for human error or deception

DON'T WAIT for a breach to occur



BE PROACTIVE… create a plan, practice and develop muscle memory

Edelman DATA SECURITY & PRIVACY GROUP 8

PREPARATION IS KEY

Proactive steps to take:

- Identify internal and external crisis team
- Keep the team lean and empower a decision-maker
- Meet your state's legislators, regulators and policy makers
- Determine your lobbying, forensics and legal firm before a crisis
- Conduct a mock crisis situation
- Develop communications chain of command for multiple scenarios

Edelman DATA SECURITY & PRIVACY GROUP 6

THE EARLY BIRD DOESN'T ALWAYS CATCH THE WORM

Move quickly, but remember that going out with information too early can hurt an organization in a data breach

- Resist communicating numbers early in the investigation; offer a timetable for additional information
- Be careful of claiming the issue is fully resolved; acknowledge that the situation may change
- Focus initial messages on the steps being taken to investigate the issue

"Facts" are very fluid - so rushing public statements can result in several bad outcomes for a company:

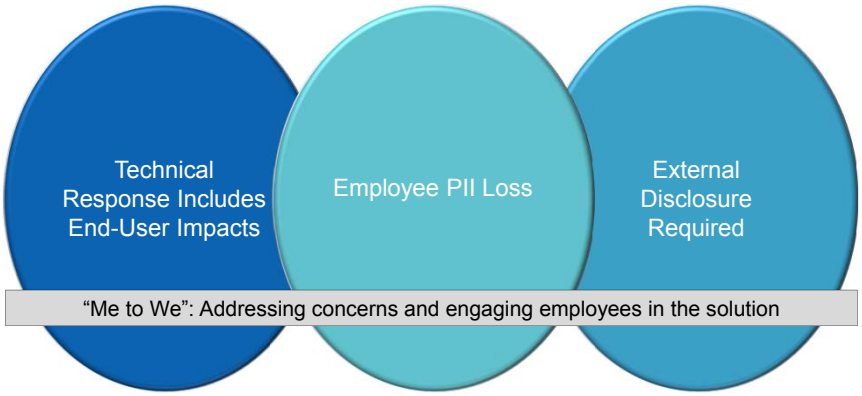
- Inaccurate dissemination of information
- Compromising more data
- Damaging company reputation further by breaking trust again

MANAGING THE MESSAGE

Customers must be your north star, so make sure that you communicate with them clearly and effectively through traditional and digital channels.

- However, don't neglect the wide variety of stakeholders interested in breaches including policymakers, regulators (state and federal) and industry stakeholders (e.g., payment brands)
- Be accountable. Take ownership and don't play the victim. Express regret.
- Be lean, but integrate legal, IT, PR and business group into communications planning
- Think through what you push out via social media
- Set up the appropriate media/social monitoring and listening posts
- Media-train executives
- Develop a long-term reputation recovery strategy, versus treating it as an isolated incident

EMPLOYEES ARE YOUR MOST CREDIBLE SPOKESPERSONS, KEEP THEM INFORMED



"Me to We": Addressing concerns and engaging employees in the solution

Edelman DATA SECURITY & PRIVACY GROUP

9