Managing Cybersecurity: An In-House Perspective

2020 Essential Cybersecurity Law

haynesboone

© 2020 Haynes and Boone, LLF

1

The Panel

- Kate Eguchi Panelist
 - Vice President and Associate General Counsel of Privacy, Marketing & Technology at Whole Foods Market
- Allan M. Johnson Panelist
 - Assistant Vice President—Senior Legal Counsel, Privacy at AT&T
- Emily Westridge Black Moderator
 - Partner, Haynes and Boone, LLP

haynesboone

© 2020 Haynes and Boone, LLF

Cyber Crime is Widespread

Over **146 billion records** are expected to be exposed through data breaches between 2018 to 2023.



73% of organizations are considered cyber novices. Only 11% are considered cyber experts.



61% of data breach victims in 2017 were **businesses with under 1,000 employees**.



The global average cost of a data breach in 2018 is \$3.86 million. For US companies, it's \$7.91 million.



Email is responsible for **92%** of malware infections through **phishing scams**.



64% of customers say they're unlikely to do business with a company that has experienced a sensitive data breach in the past.



Organizations face an average cost of \$2.8 million when they lose 1% or less of customers as a result of a breach.



On average, **68% of breaches** took months or longer to discover.



Source: Cybersecurity Statistics in 2019; TitanFile Inc.

haynesboone

© 2020 Haynes and Boone, LLP

3

Topics

- 1. Effective internal controls (including in WFH environments)
- Educating and protecting your board
- Managing vendor risk
- 4. Incident response plans
- Forensic investigations and privilege
- 6. Other incident response considerations
- 7. Resources to keep you up to date

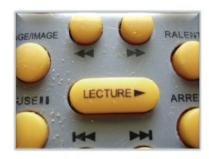


haynesboone

© 2020 Haynes and Boone, LLI

1. Effective Internal Controls

- Developing the right policies and procedures
- Training on security and awareness
- Improving technical controls
- Performing behavior analytics and risk assessment
- Communicating regularly with IT



haynesboone

© 2020 Haynes and Boone, LLP

5

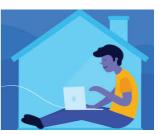
1. Internal Controls for Remote Work

- Education and training updates
- Keep employees engaged
 - Team training
 - Phishing exercises
- Monitor data flow
 - *E.g.*, are people sending secure data to personal accounts?
- No one-size-fits-all solutions
 - Adjust protocols based on duties and needs
 - E.g., management vs. call center employees vs. interns



This Photo by Unknown Author is licensed under CC BY-SA

© 2020 Haynes and Boone, LLP







Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the <u>UT Law CLE eLibrary (utcle.org/elibrary)</u>

Title search: Managing Cybersecurity: An In-House Perspective

Also available as part of the eCourse <u>2020 Challenges in Confronting Cyber Threats: Emerging Technology plus an In-</u> House Perspective

First appeared as part of the conference materials for the 2020 Essential Cybersecurity Law session "In-House Counsel Panel"