

# 8 Questions Your Board Will Ask About Digital Risk

Cyber risk accountability is moving up the org chart and into the boardroom. Executives and board members are becoming increasingly cyber savvy—and looking for exec colleagues with risk management or security experience. Investors are also demanding that companies provide clear digital risk management strategies, including showing the business impact of digital risk on both brand and reputation.

Here are the eight critical risk questions RSA predicts your board members are most likely to ask. Are you prepared to answer?

91% of organizations with \$1B+ annual revenue have BRIEFED THEIR BOARDS on their cybersecurity programs AT LEAST ONCE IN THE LAST YEAR<sup>1</sup>

## 1 Are we at risk for a cyber attack?

How does your company rank cybersecurity capabilities, including threat detection and response, security monitoring, identity management and vulnerability management?



30% of companies have experienced a **DATA BREACH** in the past year<sup>2</sup>

## 2 Are we doing enough to secure our workforce?

Is your workforce global, remote or dynamic? Cloud applications, a growing number of endpoints, and differing regional data and privacy requirements make access control and identity management more challenging.

### TOP 3 WORKFORCE SECURITY CHALLENGES<sup>3</sup>

Increased reliance on cloud-based applications

Technology-based knowledge gaps

Data and privacy requirements

## 3 How will cloud transformation affect us?

Do you thoroughly vet cloud providers' security, privacy and compliance practices? Do you have the proper governance and access controls to manage all of your cloud service providers?



40% of organizations plan to spend all **NEW OR ADDITIONAL FUNDING ON CLOUD INITIATIVES**<sup>4</sup>

## 4 How well do we manage third-party risk?

Digital transformation expands third-party relationships, making them more complex and difficult to manage. How well do you identify and manage security, access, compliance, resiliency and other risks stemming from third-party partners?

### TOP 3 THIRD-PARTY RISKS<sup>5</sup>



Cyber attack/  
data breach



Privacy  
violations



Operational  
disruption

## 5 Can we afford the cost of compliance?

The real question is the cost of noncompliance. Data protection and privacy regulations, including GDPR and CCPA, levy substantial fines for noncompliance.

## 6 How well do we protect our customers' data?

4 **COSTS OF NONCOMPLIANCE**<sup>6</sup>

1. Business disruption
2. Productivity loss
3. Revenue loss
4. Fines and penalties

95% of companies say regulations **WILL INCREASE THEIR COMPLIANCE COSTS IN 2020**<sup>7</sup>



Companies that have **EXPERIENCED A BREACH UNDERPERFORM THE MARKET** by more than **13%** three years later<sup>8</sup>  
**9 BILLION** compromised accounts in 2019<sup>9</sup>

## 7 Are we using AI to minimize digital risks?

The deeper we dive into the IoT, the more organizations look to AI to raise productivity, improve sales and enhance customer experience. But AI can also shore up defenses against the digital risks that inevitably follow.

**69%** of ENTERPRISES **BELIEVE** AI will be necessary to **RESPOND TO CYBER ATTACKS**<sup>10</sup>

## 8 How good are our business continuity, disaster recovery and crisis management capabilities?

*It's not if, but when.* The likelihood of a cyber attack is a stark reality. Are you taking a preventative or a resilient approach? How well could you manage an attack while reducing risk exposure?



**UNPLANNED DOWNTIME COSTS** small to medium size companies an average of **\$125K PER EVENT—AS MUCH AS \$17M+ PER EPISODE** for large enterprises<sup>11</sup>

Assess your top digital risks in minutes with the **RSA® Digital Risk Index** and learn how to answer these questions in our report, **How to Talk Digital Risk to the Board.**

Sources: 1. Gartner, Five Board Questions That Security and Risk Leaders Must Be Prepared to Answer, July 2019. 2. IDC, The Changing Face of Data Security, 2019 Global Edition. 3. SANS Institute, Workforce Transformation and Risks: A SANS Survey, December 2019. 4. Gartner, Top 7 Security and Risk Management Trends, January 2019. 5. Forrester Research, December 2019. 6. Ponemon Institute, True Cost of Compliance with Data Protection Regulations, 2018. 7. Duff & Phelps, Global Regulatory Outlook, 2018. 8. Paul Bischoff, How data breaches affect stock market prices, comparitech, November 2019. 9. haveibeenpwned? website, December 2019. 10. CapGemini, Reinventing Cybersecurity with Artificial Intelligence, July 2019. 11. Evolve IP, IDC: Statistics on the Financial Impact of Unplanned Downtime, August 2017.