In 2015, 5 TRILLION DOLLARS was tied up in merger and acquisition deals due to cybersecurity issues.\(^1\)

85% of directors said the discovery of a major cybersecurity vulnerability would impact their decision on a merger or acquisition (M&A).\(^2\)

31% of impacted organizations reported that security incidents caused downtime of more than eight hours.\(^3\)

87% of U.S. business executives are worried that cyber threats could have an impact on their company’s growth prospects.\(^4\)

54% of IT professionals polled said their company experienced at least one security incident caused by human error or recklessness.\(^5\)

52% of the organizations that experienced a cyberattack in 2016 aren’t making any changes to their security in 2017.\(^6\)

40% of corporate executives said they’re not responsible for the repercussions of hacking.\(^7\)

65% of companies are considering different ways to collaborate with their suppliers to mitigate risks.\(^8\)

Companies doing business in Europe that aren’t compliant can face a penalty equal to 4% of their gross worldwide revenue.\(^9\)

87% of bank and capital markets CEOs are concerned about over-regulation.\(^10\)

Only 40% of healthcare professionals were confident their organization would remain HIPAA-compliant.\(^11\)

61% of retail organizations strongly agree that they’ll be able to maintain the full Payment Card Industry Data Security Standard (PCI-DSS).\(^12\)

40% of U.S. imports came from countries with a high risk of natural disaster exposure.\(^13\)

SEE THE NEED FOR BUSINESS-DRIVEN SECURITY SOLUTIONS? RSA ARCHER® HELPS YOU KNOW WHICH RISK IS WORTH TAKING. LEARN MORE AT RSA.COM

OPERATIONAL RISK

85% OF DIRECTORS said the discovery of a major cybersecurity vulnerability would impact their decision on a merger or acquisition (M&A).1

In 2015, 5 TRILLION DOLLARS was tied up in merger and acquisition deals due to cybersecurity issues.2

SECURITY RISK

31% OF IMPACTED ORGANIZATIONS reported that security incidents caused downtime of more than eight hours.3

87% OF U.S. BUSINESS EXECUTIVES are worried that cyber threats could have an impact on their company’s growth prospects.4

54% OF IT PROFESSIONALS polled said their company experienced at least one security incident caused by human error or recklessness.5

52% OF THE ORGANIZATIONS that experienced a cyberattack in 2016 aren’t making any changes to their security in 2017.6

40% OF CORPORATE EXECUTIVES said they’re not responsible for the repercussions of hacking.7

COMPLIANCE RISK

87% OF BANK AND CAPITAL MARKETS CEOs are concerned about over-regulation.8

ONLY 40% OF HEALTHCARE PROFESSIONALS were confident their organization would remain HIPAA-compliant.9

ONLY 61% OF RETAIL ORGANIZATIONS strongly agree that they’ll be able to maintain the full Payment Card Industry Data Security Standard (PCI-DSS).10

Companies doing business in Europe that aren’t compliant can face a penalty equal to 4% OF THEIR GROSS WORLDWIDE REVENUE.12

SUPPLY CHAIN RISK

65% OF COMPANIES are considering different ways to collaborate with their suppliers to mitigate risks.10

NEARLY 40% OF U.S. IMPORTS came from countries with a high risk of natural disaster exposure.17