RSA

SEE THE NEED FOR **BUSINESS-DRIVEN SECURITY™ SOLUTIONS?**

GET TO KNOW RSA. AND YOU'LL **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 the'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).[11]

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.[13]

Sources: 1. Cyberttoa. *Cybersecurity during a merger or acquisition.* 2. Fireeye. *Unsealing the deal: Cyber threats to mergers and acquisitions persist in a hot market.* 3. Net IQ. *84 fascinating & scary IT security statistics.* 4. AT&T. *What every CEO needs to know about cybersecurity.* 5. Cisco. *Cybersecurity professionals on the current state of cybersecurity.* 6. Barkly. *6 must-know cybersecurity statistics for 2017.* 7. CNBC. *Execs: We're not responsible for cybersecurity.* 8. CDW FinTalk. *A secure path to regulatory compliance.* 9. Linkedin Pulse. *10 Eye-Opening Healhtcare Statistics.* 10. Resolver. *Natural disasters and their impact on supply chains.* 11. Cisco. *Keeping up with cybersecurity threats in the digital age.* 12. Cybersecurity Ventires. *Governance, Risk & Compliance (GRC) Report.* 13. BSI Supply Chain. *Natural disaster–supply chain risks.*

RSA

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 the'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).[11]

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.[13]

Sources: 1. Cyberttoa. *Cybersecurity during a merger or acquisition.* 2. Fireeye. *Unsealing the deal: Cyber threats to mergers and acquisitions persist in a hot market.* 3. Net IQ. *84 fascinating & scary IT security statistics.* 4. AT&T. *What every CEO needs to know about cybersecurity.* 5. Cisco. *Cybersecurity professionals on the current state of cybersecurity.* 6. Barkly. *6 must-know cybersecurity statistics for 2017.* 7. CNBC. *Execs: We're not responsible for cybersecurity.* 8. CDW FinTalk. *A secure path to regulatory compliance.* 9. Linkedin Pulse. *10 Eye-Opening Healhtcare Statistics.* 10. Resolver. *Natural disasters and their impact on supply chains.* 11. Cisco. *Keeping up with cybersecurity threats in the digital age.* 12. Cybersecurity Ventires. *Governance, Risk & Compliance (GRC) Report.* 13. BSI Supply Chain. *Natural disaster–supply chain risks.*