Concern about cybersecurity is ubiquitous in today’s corporate world. Our second annual RIMS Cyber Survey highlights the measures that an increasing number of organizations are relying on, while also showing that opinions are far from aligned on reporting requirements.

As far as handling cyber exposure, this year’s survey saw a leap in the number of organizations who are transferring the risk. Nearly 70% reported some form of transfer, an increase of 10% over 2015. Stand-alone cyber insurance policies seem to be the preferred route: a resounding 80% of survey respondents reported purchasing this type of cover, an increase of 29% compared to the 2015 collection.

Many organizations are being pushed in this direction by multiple forces. For example, a quarter of respondents said that they are required to buy cyber insurance as a result of contractual obligations, a leap of 17% from 2015. Here we can see evidence of organizations with large supply chains pressuring their vendors to increase their cybersecurity.

Premium paid for coverage varies widely. That said, nearly a quarter of respondents said they are paying more than $500,000 for their policies.

Regulators and legislators in many countries have been debating whether or not to mandate and standardize cyber breach reporting. Among our U.S. respondents, opinions of this approach are split: 48% think that the federal government should mandate reporting, while the rest are opposed or unsure. Meanwhile, there seems to be a lack of familiarity among risk managers about information sharing and analysis organizations (ISAO) that were created by federal legislation in 2015. Only 20% could confirm that their organizations were participating, and 40% confirmed that their companies were not.

The world of cybersecurity is, of course, rapidly evolving. That is also true for the insurance and risk management components. Please visit RIMS resources such as Risk Management Magazine, Risk Knowledge database, courses and webcasts to stay in the loop.

**METHODOLOGY**

This year’s survey had 272 respondents; 2015 had 284. Demographics such as industry sector, organization revenue and number of employees held close to 2015 results. The survey was distributed to RIMS membership via an internet link, and was in field between August 8 and September 9, 2016. If you have additional questions about data collection, please contact RIMS at content@rims.org.

As the preeminent organization dedicated to educating, engaging and advocating for the global risk community, RIMS, the risk management society™, is a not-for-profit organization representing more than 3,500 corporate, industrial, service, nonprofit, charitable and government entities throughout the world. RIMS has a membership of approximately 11,000 risk practitioners who are located in more than 60 countries. For more information about the Society’s world-leading risk management content, networking, professional development and certification opportunities, visit www.RIMS.org.
### Survey at a Glance

- **Organizations transferring the risk of cyber exposure to a third party**
  - Up 10% from 2015 to 2016
- **Organizations with a stand-alone cyber insurance policy**
  - Up 29% from 2015 to 2016
- **Organizations purchasing cyber insurance as a result of contractual obligations**
  - Up 17% from 2015 to 2016

- **Nearly a quarter of respondents are spending over $500,000 on cyber premiums.**
- **Fewer than 50% of risk managers think the government should mandate cyber breach reporting.**
- **Only 20% of respondents say their organizations are part of ISAOs.**
QUESTION 1. What are your organization’s potential first-party cyber exposures:

- Business interruption and extra expense as a result of network outage: 76%
- Business interruption and extra expenses for loss of data: 75%
- Cyber extortion: 63%
- Theft of trade secrets or IP: 42%
- Reputational harm: 82%
- Regulator investigations, fines, penalties: 65%
- Costs related to notification, response, etc.: 76%}

QUESTION 2. What are your organization’s potential third-party cyber exposures:

- Disclosure of personal identifiable information (employees or customers/suppliers): 85%
- Media liability: 38%
- Business interruption: 57%
- Economic harm to customers as the result of a network outage: 51%
- Regulator investigations, fines, penalties: 60%
- Costs related to notification, response, etc.: 69%
**QUESTION 3.** Does your organization transfer the risk of cyber exposure to a third party?

- Yes: 69% (▲10% from 2015)
- No: 24%
- Not sure: 7%

**QUESTION 4.** Is your organization considering a purchase of cyber coverage within the next 12-24 months?

- Yes: 67%
- No: 14%
- Not sure: 19%

**QUESTION 5.** Does your company have a stand-alone cyber insurance policy?

- Yes: 80% (▲29% from 2015)
- No: 19.5%
- Not sure: 0.5%
**QUESTION 6.** Does your organization purchase cyber insurance as a result of contractual obligations?

- Yes: 25% (▲17% from 2015)
- No: 74%
- Not sure: 1%

**QUESTION 7.** What is the range of limit purchased?

- Less than $5 million: 20.5%
- $5 million-$20 million: 38.5%
- $20 million-$50 million: 13.5%
- $50 million-$100 million: 15.5%
- $100 million-$200 million: 8%
- More than $200 million: 3.5%
QUESTION 8. What premium are you paying for your cyber coverage?

- Less than $50,000: 24%
- $50,000-$75,000: 12.5%
- $75,000-$100,000: 10.5%
- $100,000-$200,000: 13.5%
- $200,000-$500,000: 16%
- More than $500,000: 23%

QUESTION 9. Which of the following is included in your cyber insurance policy?

- Professional liability: 50%
- Network/business interruption: 76%
- Cyber extortion: 78%
- Fines and penalties: 63%
- Breach notification costs: 91%
- Reputational harm: 42%
- Theft of trade secrets: 27%
- Data recovery: 80%
**QUESTION 10.** Does your organization’s cyber insurance coverage extend to data stored in cloud servers?

- Yes: 69%
- No: 9%
- Not sure: 22%

**QUESTION 11.** Does your organization have a response plan in place in the event of a cyber crisis?

- Yes: 81%
- No: 7%
- Not sure: 12%
QUESTION 12. Who is involved in that response procedure?

- Public relations: 75%
- Information technology: 94%
- Legal: 85%
- Risk management: 84%
- Information security: 82%
- Compliance: 52%
- Privacy officer: 47%

QUESTION 13. Has your organization identified cyberrisk using any of the following methods or tools?

- Enterprise risk management (ERM): 49%
- Strategic risk management (SRM): 22%
- Software: 28%
- Consultants: 53%
- Not sure: 19%
QUESTION 14. Which of the following has primary responsibility for cybersecurity within your organization?

- Risk management: 5%
- Information security: 42%
- Information technology: 47%
- Privacy: 2%
- Compliance: 3%

QUESTION 15. Which individual within your company has primary accountability for cybersecurity?

- Risk manager: 5%
- Chief information security officer: 84%
- Chief risk officer: 2%
- Chief privacy officer: 3%
- Chief compliance officer: 3%
- Attorney: 4%
QUESTION 16. Which of the following methods does your company use to evaluate cybersecurity?

- In-house committee: 62%
- Third party vendor: 61%
- Risk assessments: 73%
- Audit: 56%

QUESTION 17. How much will your company spend to protect cybersecurity exposures in 2016?

- Less than $100,000: 23%
- $100,000-$250,000: 19%
- $250,000-$500,000: 18%
- $500,000-$750,000: 9%
- $750,000-$1 million: 7%
- More than $1 million: 24%
QUESTION 18. What will be your top cyberrisk spending categories in 2016?

- Employee education: 46%
- Incident response: 27%
- Scanning tools: 47%
- Smart phone encryption software: 15%
- Active monitoring and analysis of information security: 75%
- Cyber insurance: 55%
- Unauthorized use of access monitoring tools: 31%
- Other: 9%

QUESTION 19. Which aspect of cyberrisk is most relevant to your company?

- Privacy issues: 26% (▲10% from 2015)
- Loss of business: 3%
- Reputational issues: 23%
- Business interruption: 23%
- Legal liability, fines, penalties: 14%
- Information security requirements: 10%
- Other: 1%
QUESTION 20. Do you think the federal government should mandate the reporting of cyber breaches? (U.S. respondents only)

- Yes: 48%
- No: 27%
- Not sure: 25%

QUESTION 21. Does your organization belong to an information sharing and analysis organization (ISAO) as created by the U.S. Cybersecurity Information Sharing Act of 2015?

- Yes: 20%
- No: 40%
- Not sure: 40%
QUESTION 22. What is your industry sector?

![Bar chart showing industry sector distribution]

- Retail: 4%
- Hospitality: 4%
- Health care: 8.5%
- Financial services: 14%
- Professional services: 5.5%
- Utilities: 4%
- Energy: 4.5%
- Government or non-profit: 10.5%
- Information technology: 3%
- Telecommunications: 1.5%
- Education: 5%
- Manufacturing: 10.5%
- Industrial: 0.5%
- Transportation: 3.5%
- Other: 21%
QUESTION 23. What is your organization’s estimated annual revenue? (USD)

- $0 to $1 million: 1.5%
- $1 million to $10 million: 2%
- $10 million to $50 million: 5%
- $50 million to $100 million: 6.5%
- $100 million to $500 million: 18%
- $500 million to $1 billion: 10.5%
- $1 billion+: 56.5%

QUESTION 24. How many total employees are in your organization?

- 0 to 100: 3%
- 100 to 250: 5%
- 250 to 500: 5.5%
- 500 to 1,000: 8%
- 1,000 to 5,000: 29.5%
- 5,000 to 10,000: 12%
- 10,000 to 15,000: 8%
- 15,000 to 25,000: 7%
- 25,000 or more: 22.5%