Risk Cooperative

CYBER 360°

Survey Overview

Agenda

01 About Risk Cooperative

02 Cyber Survey Highlights

03 Risk, Readiness, Resilience

04 Questions?

01

ABOUT

A key focus area for Risk Cooperative is emerging risks, cyber being the top concern.

- Founded in 2014
- Robust employee benefits practice, including group disability, key life and retirement planning
- Extensive expertise across all classes of insurance including, life, health, property, casualty, specialty risks as well as excess and surplus lines of insurance
- Licensed nationally across all 50 states, Puerto Rico and Washington, D.C.
- Global coverage capabilities
- Offices in Washington D.C.

02

SURVEY

Prior Year Cyber 360° Survey Highlights

The **360° Cyber Survey** was designed to help business leaders go beyond baseline compliance and technical components to help evaluate their overall business resiliency to cyber threats.

The report not only provides a detailed overview of the responses, but also analysis from cyber and risk experts and actionable recommendations to help guide members through mitigation steps to improve their cyber resiliency.

02

SURVEY

Prior Year Cyber 360° Survey Highlights

Survey respondents represented various industries across public and private sectors. The majority of respondents (33.9%) were in the government contracting industry, followed by professional services (19.6%), and technology (16.1%). Since most of the companies that participated in the survey are based in the Washington DC Metro area, it is not surprising that the top three industries represented in the survey are reflective of the key players in the regional economy.

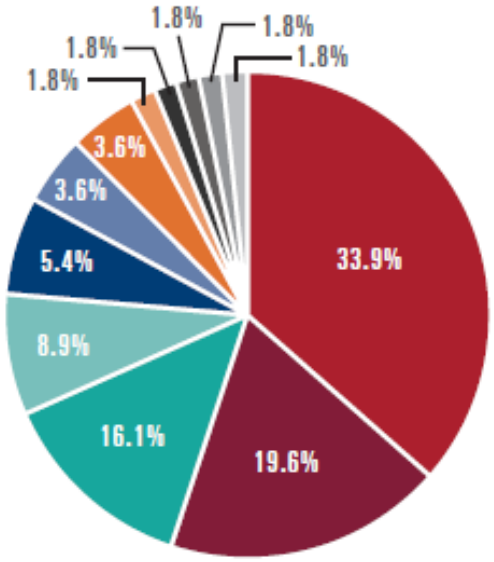


Figure 2: Survey Respondent Industries

- Government Contractors
- Professional Services
- Technology
- Non-Profit
- Financial Services
- Health Care
- Insurance
- Education
- Infrastructure & Logistics
- Energy
- Public Sector
- Real Estate

02

SURVEY

Prior Year Cyber 360° Survey Highlights

SURVEY INSIGHTS

58.9%

Of survey respondents had more than 50% of cybersecurity preparedness activities included within their operational responsibilities.

ACCOUNTABILITY & COORDINATION

Cyber risks have enterprise-wide impacts. Therefore, the success of a cybersecurity program is highly dependent upon a supported organizational structure where leaders are clearly assigned and held accountable. In organizations with successful cybersecurity programs, coordination is encouraged and achieved to optimize outcomes.

33.3%

Of the respondents reported that overall accountability for cybersecurity initiatives was held by the Chief Executive Officer (CEO)

27.5%

Of respondents noted these groups do not coordinate

25.9%

Followed by the IT Department Manager

20.4%

Chief Information Security Officer (CISO) / Chief Security Officer (CSO)

While the oversight of cybersecurity initiatives is primarily managed by a CEO or IT leader, the success of these efforts depends on other key department leads, including the legal department. For some larger organizations a General Counsel or legal support may be in-house, but for some smaller organizations they may require support from outside counsel.

02

SURVEY

Prior Year Cyber 360° Survey Highlights

Education

Education and training are crucial to protect against information & asset security incidents. However, 36.4% of respondent noted their organizations did not conduct security awareness training. Of those who did deliver this training, it was most commonly conducted annually (38.6%). Role-based training was conducted predominantly on an ad hoc basis (43.5%), followed by not being conducted at all (37%), annually (13%), and semi-annually (6.5%).

SECURITY AWARENESS TRAINING IS INTENDED TO BE APPLICABLE TO ALL PERSONNEL BY INFORMING THEM OF THEIR RESPONSIBILITIES TO PROTECT ORGANIZATION ASSETS. THIS ALSO INVOLVES CONTINUING EDUCATION ON CURRENT TRENDS AND WAYS TO COUNTER CYBER THREATS (E.G., PHISHING EMAILS, VIRUSES, AND RANSOMWARE). THIS TRAINING IS ESSENTIAL TO CULTIVATING A SECURITY RISK AWARE CULTURE. HOWEVER, IT ALONE IS INSUFFICIENT FOR VARIOUS ROLES ESPECIALLY WITHIN THE IT DEPARTMENT. DUE TO EVOLVING NATURE OF CYBER RISKS AND A LACK OF ADEQUATE RESOURCES, MOST ORGANIZATIONS CONDUCT AD HOC TRAINING. HOWEVER, THE REALITY IS THAT IN THE 21ST CENTURY RISK ENVIRONMENT, ALL ROLES, INCLUDING SENIOR LEADERS IN THE C-SUITE AND BOARD, SHOULD HAVE PERIODIC TRAINING. WHILE NOT THE ONLY SOLUTION, IT CAN OFTEN BE A LOW COST AND HIGHLY EFFECTIVE MEASURE TO LIMIT CYBER RISK.

How often is security awareness training conducted? Security awareness training includes topics such as IT policies and procedures, incident management, and reporting.

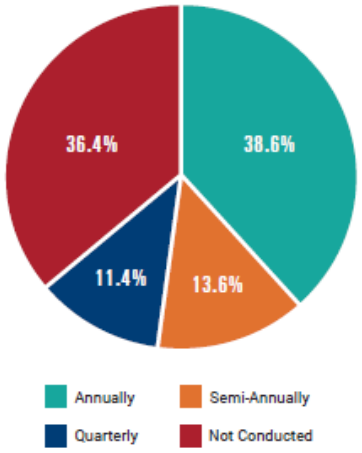


Figure 2: *Security Awareness Training Frequency*

55%

Of respondents have NOT identified the sensitive information within their organization.

59.6%

A majority of respondents indicated that less than 25% percent of their business operations were dependent on sensitive data such as personally identifiable information (PII).

86.7%

Of respondents indicated using network security devices such as intrusion prevention technology to safeguard information.

02

SURVEY

Prior Year Cyber 360° Survey Highlights

46.5%

Of respondents noted that Business Continuity/ Disaster recovery plans were finalized and disseminated to relevant stakeholders.

46.5%

Did not have these plans finalized and distributed.

7%

Of respondents were unaware of such documentation.

Have the Business Continuity / Disaster Recovery plans and procedures been tested to validate their effectiveness?

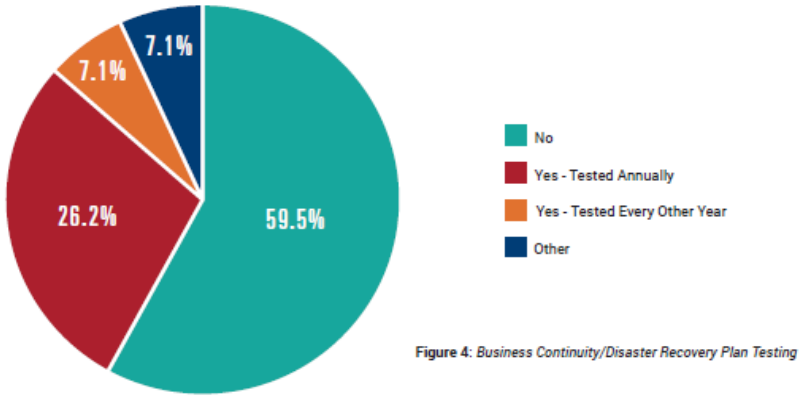


Figure 4: *Business Continuity/Disaster Recovery Plan Testing*

02

SURVEY

Prior Year Cyber 360° Survey Highlights

Of the survey respondents,

41.9%

indicated that they had some sort of cyber liability insurance in place at their organizations.

This is a positive indication that survey participants are forward thinking in how they can build up their organizations' overall resiliency and cybersecurity. Yet, cyber insurance remains a highly underutilized tool when it comes to cybersecurity. This is largely due to a great deal of discrepancies in the insurance markets and confusion among the available insurance products.

Of all the cyber insurance policies in effect,

95%

are bundled policies.

This means the cyber policy is an add-on to another class of insurance, most often a general liability or business owners' policy.

5%

of policies are what is called a standalone policy, which offers more robust coverage and protection for cyber risk on a "first dollar basis."

Against this backdrop, it is not surprising that

47.2%

of respondents noted that it was not applicable to their organization.

03 Risk, Readiness, Resilience

RISK

Remote work has increased the risk of cyber breaches

In malicious domains related to COVID-10

In domains that send email phishing campaigns

Geopolitical tensions have weaponized cyber attacks

U.S. intelligence agencies attributed the **sophisticated Solarwinds malware campaign to Russia**

Killing of Iranian General Soleimani and scientist Mohsen Fakhrizadeh are examples of potential retaliation via cyber attacks against military and civilian assets.

Hospitals and pharmaceutical companies combating COVID-19 have been victims of cyber attacks.

Questions for InfraGard Members

- Who at your organization is responsible for your cybersecurity program?
- Do you employ a Chief Information Security Officer (CISO) or a similar C-Level exec in charge of cybersecurity matters?
- Has your organization developed and shared cyber policies and procedures?
- How do you test your cyber risk mitigation program?
- What is your cyber requirement for venders and service providers?

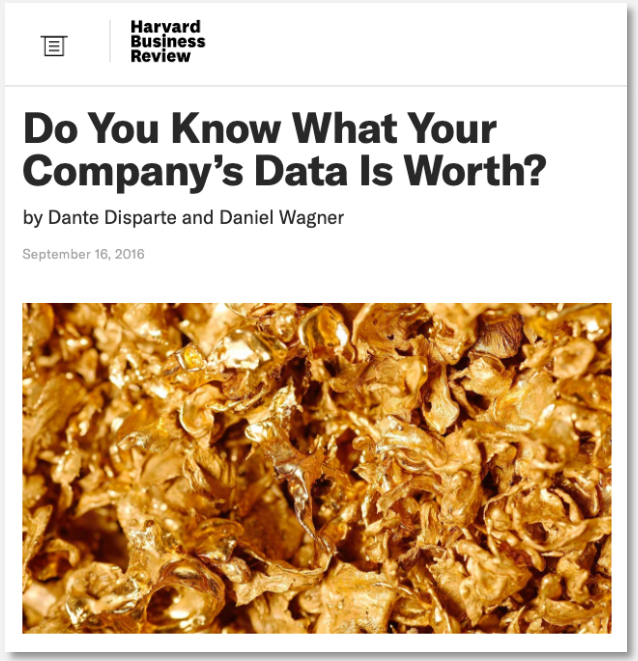
03 Risk, Readiness, Resilience

READINESS

Companies must be aware of the value of their data, so in case they experience a breach they will have an understanding of revenue at risk

The greatest risk lies between the keyboard and the chair, and cyber hygiene training has proven to be the most effective tool to combat phishing attacks and other forms of social engineering

Companies must have their policies and procedures in place, as well as their Cyber Response plan in preparation for a cyber attack



Questions for InfraGard Members

- What safeguards are in place to protect sensitive information?
- Do you routinely conduct organization-wide and role-based security/hygiene trainings?
- Do you have appropriate event detection measures in place to alert you to an incident?
- Does your team know how to respond when an incident is discovered?

03 Risk, Readiness, Resilience

RESILIENCE

"Tone from the top" mentality must be established.

Board oversight is key to ensure that a cyber hygiene, and recovery, strategy is in place.

Companies must be aware of important policy declarations in their cyber policies which can have an even greater impact during this high-risk environment.

- War Exclusion
- Prior Coverages
- Bodily Injury & Property Damage resulting from cyber incident

Questions for InfraGard Members

- Has the organization quantified its cyber risk threshold?
- Do you have a response team in place?
- How will you communicate with your clients and vendors?
- What resources can help with the financial impact of a breach?
- If your organization has a board of directors, is there at least one director who has an IT background?

04

Questions?

04
RESOURCES

Linked Resources

Click on each link or button to open.

🔗 Executive Briefing on Cyber Insurance

🔗 Coronavirus and Telecommuting: How One Risk Is Giving Way to an Even Bigger Challenge (Risk & Insurance)

🔗 Innocent Cyber Bystanders Entangled in an Act of War (International Policy DIgest)

🔗 Do You Know What Your Company's Data is Worth (Harvard Business Review)

🔗 Risk Matters 115 | Cyber Myths

🔗 Insurance Insights | Cyber Exclusions

Survey respondents receive a complimentary copy of the updated report containing expert recommendations, benchmarking, and best practices for cyber resiliency.

Cyber 360° Survey Link

🔗 360° Cyber Survey Report (2017)

More questions? Send us a message and we'll get you the answers you need.

Contact Us

Risk Cooperative
1825 K Street NW, Ste 1000
Washington, DC 20006

info@riskcooperative.com
P | +1.202.688.3560
F | +1 202.905.0308