Nationwide®

September 2022

Nationwide Agency Forward

Cybersecurity – Risk Management Research

METHODOLOGY

Audience

Corporate Risk Management Professionals

Corporate risk management professionals employed by mid-sized firms, defined as those reporting annual revenue of $250 million to $1.5 billion.

Sample Size

N=500

Methodology

20 - Minute Online Survey

Timing

Survey fielded August 8th – 25th, 2022

Risk Landscape

Risk managers are most concerned about IT and cybersecurity risks

Other common sources of concern are financial, compliance/regulatory, and strategic risk.

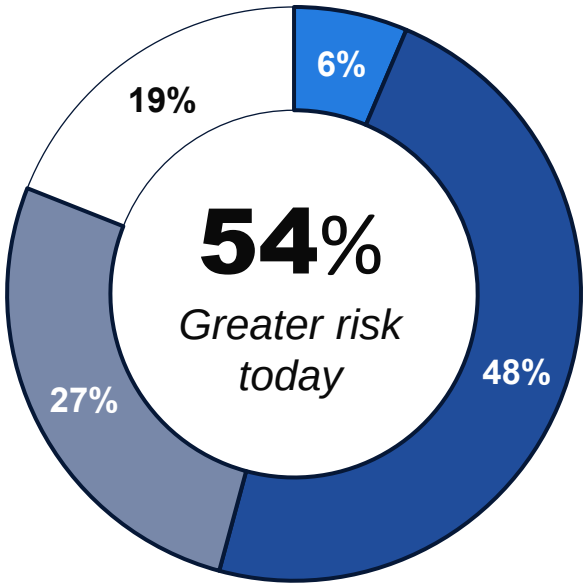
Nationwide®

Q1. Thinking about your company and your experiences in risk management, what sources of business risk are you currently most concerned about? Base: Risk Manager (Total: n=500)

Corporate cyber risk grew substantially during the pandemic and has been further heightened by the war in Ukraine

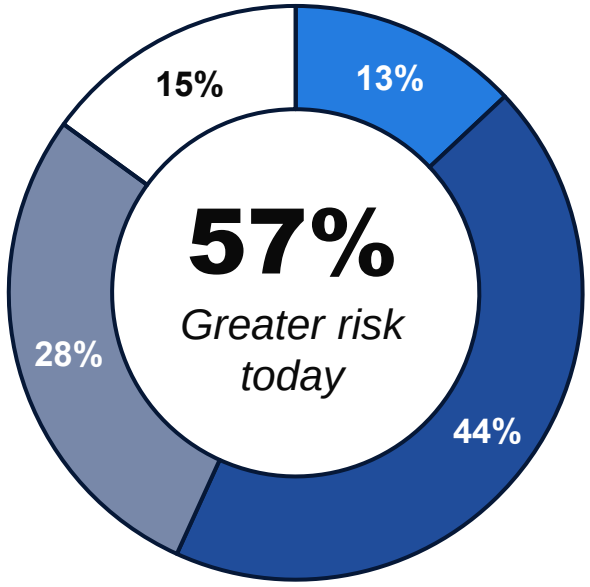
How Company Cyberattack Risk Has Changed…
(Shown % Select)

… compared to before the COVID-19 pandemic



- Much greater risk today
- Somewhat greater risk today
- There is no difference
- Less risk today

… compared to before the war in Ukraine began



Nationwide®

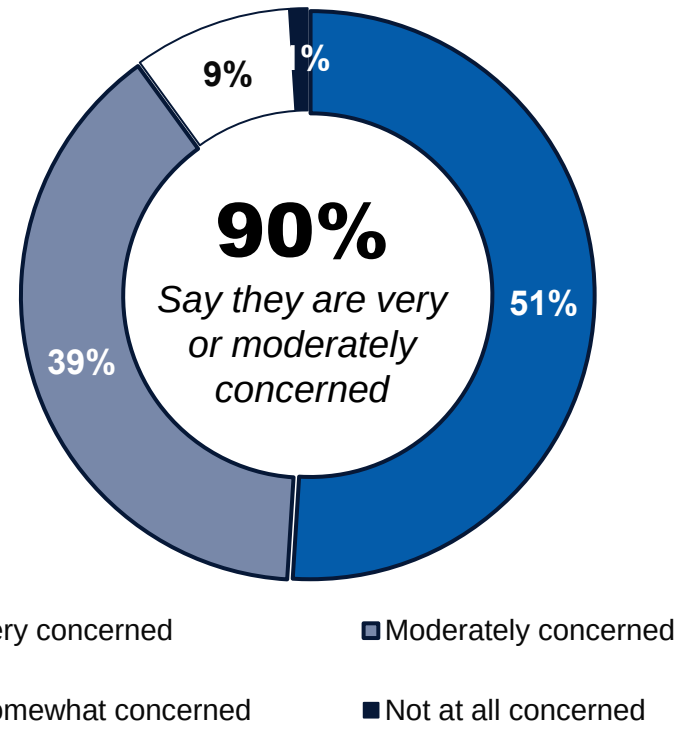
Q14. Based on your experience, how has your company's risk to cyberattacks changed compared to before the COVID-19 pandemic? Base: Risk Manager (Total: n=500)
Q15. Based on your experience, how has your company's risk to cyberattacks changed compared to before the war in Ukraine began in February 2022? Base: Risk Manager (Total: n=500)

Half of risk managers are very concerned that their company will fall victim to a cyberattack in the future

Increased frequency of attacks, technological innovations since the pandemic, and the Ukraine war are commonly cited as reasons for concern.

Concern about Potential Cyberattacks on Employer

(Shown % Select)



Reasons for Concern

(Shown: % Select, among those who are concerned about cyberattacks)

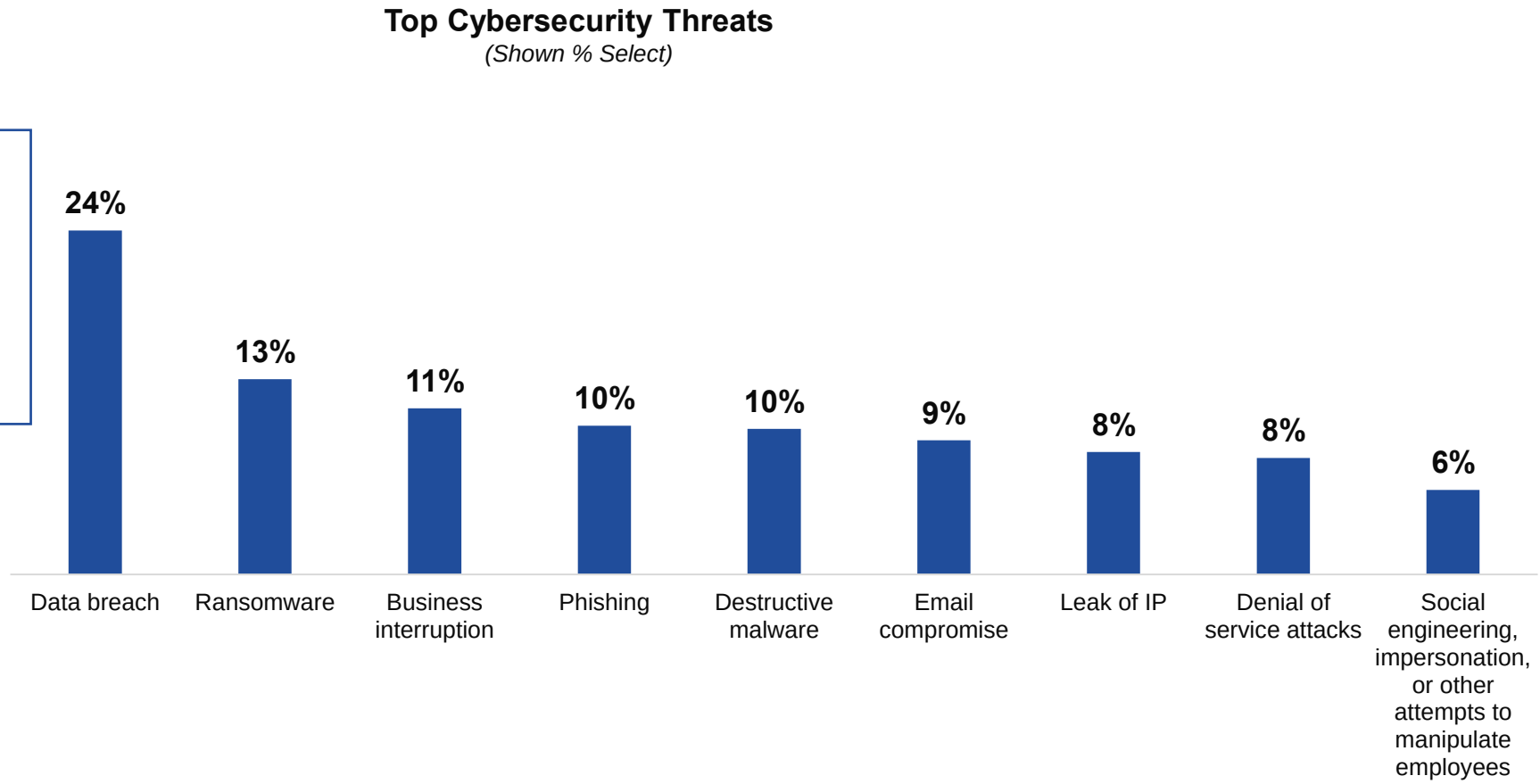
	Risk Managers
Cyberattacks have been increasingly common in the last few years	45%
The pandemic has been a catalyst for new ways to breach our system	38%
I'm concerned because of the increased potential for cyberattacks stemming from the war in Ukraine	36%
Maintenance of our IT systems is not conducted regularly enough	35%
With a digital supply chain, there are more devices than ever vulnerable to cyberattacks	35%
There are not enough IT measures in place to effectively prevent cyberattacks	35%
The data our business collects is not properly examined for cyberthreats	35%
Employees do not have adequate cybersecurity training	35%
My company does not have adequate insurance against a cyberattack	31%

Nationwide®

Q3. How concerned are you that your company can be a victim of a cyberattack in the future? Base: Risk Manager (Total: n=500)
Q4. Why are you concerned about a potential cyberattack on your company? Base: Risk Managers who are concerned about cyberattacks (Total: n=449)

Data breaches, ransomware and business interruption are seen as the top cybersecurity threats today

> *The **threats of data breach, theft, and loss** have become more prominent now due to a lack of cloud security."*
> *– Risk Manager*



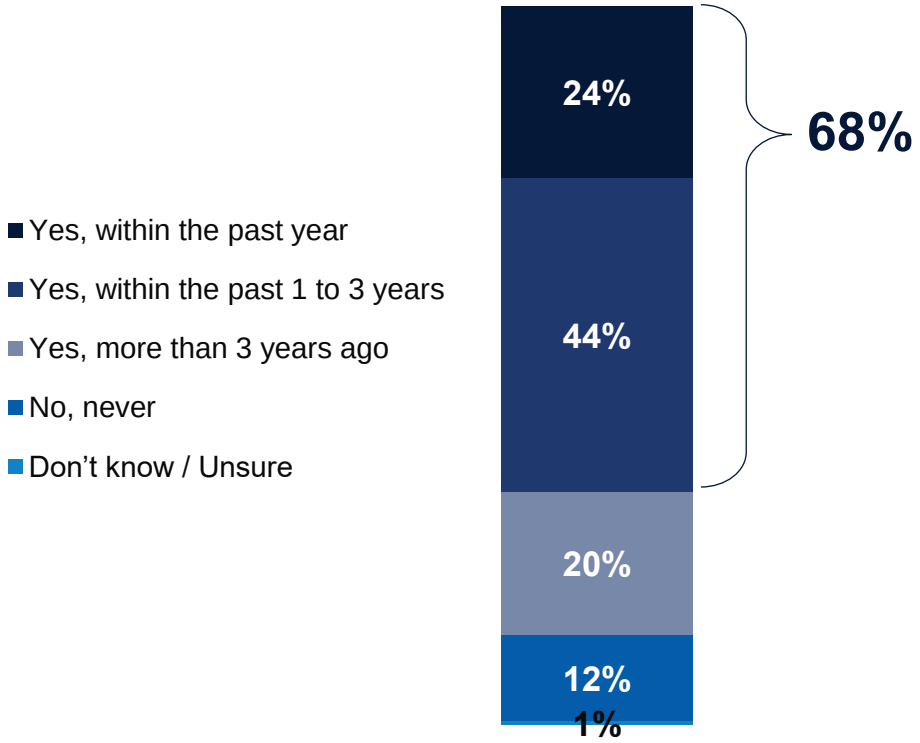
Nationwide®

Q5. Thinking about your company specifically, what type of cyberattack is your biggest concern? Base: Risk Manager (Total: n=500)

Almost 7 in 10 risk managers say they experienced a cyberattack in the past 3 years – with data breaches, destructive malware, and ransomware being the most common

Data breaches are also the top cyber threat that risk managers are concerned about.

Employer Been Victim of a Cyberattack
(Shown % Select)



Most Recent Cybersecurity Threat Experienced
(Shown % Select, among those who have experienced a cyberattack)

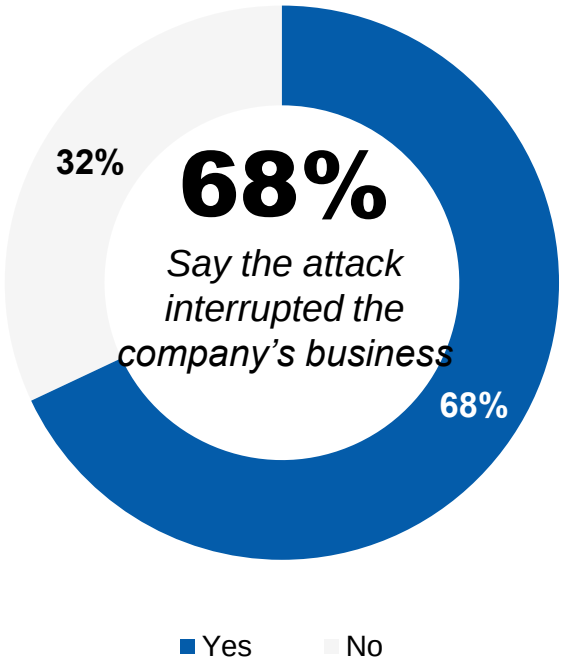
1	Data breach	23%
2	Destructive malware	10%
3	Ransomware	8%
4	Business interruption	8%
5	Leak of IP	8%
6	Phishing	8%
7	Ransomware and data breach in the same attack	7%
8	Email compromise	7%
9	Mobile POS breach	4%
10	Denial of service (DoS)	4%
11	Digital tax fraud	4%
12	Impacted by attack on the digital supply chain	4%
13	Digital unemployment fraud	3%
14	Social engineering, impersonation, or other attempts to manipulate employees	3%
15	Deepfakes	2%

Nationwide®

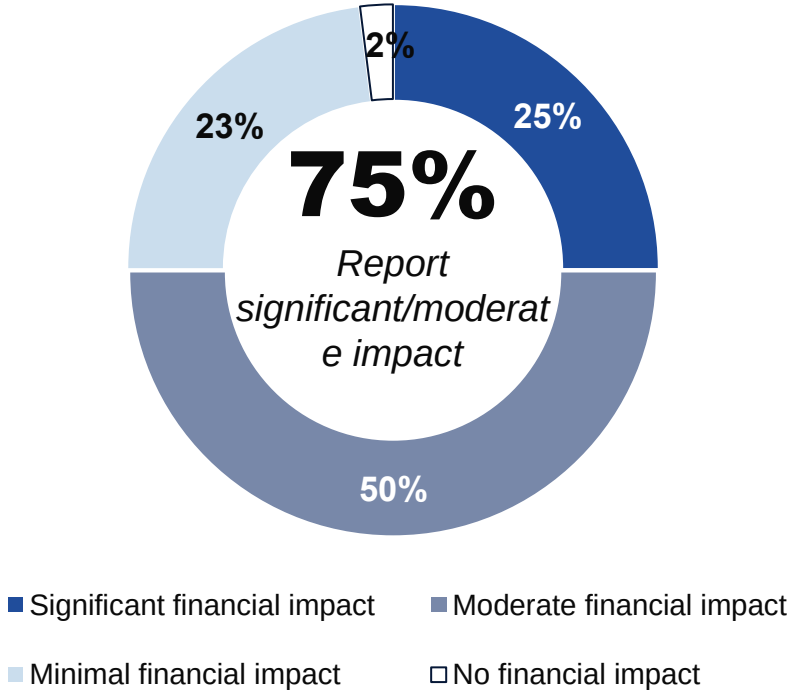
*Q10. To the best of your knowledge has your company ever been the victim of a cyberattack? A cyberattack is an unwelcome attempt to disrupt, damage, or destroy a computer system (a network of computers, smart phones, smart devices, etc.). Base: Risk Manager (Total: n=500) Q11A. What type of cyberattack did your company experience? If your company has experienced more than one attack in the past three years, please refer to the **most recent** attack. Risk Managers who have experienced a cyberattack (n=340)*

Risk managers who have experienced cyberattacks say they are disruptive and have a substantial impact on company finances

Cyberattack Impacted or Jeopardized Business Operations
(Shown % Select, among those who have experienced a cyberattack)



Cyberattack Negatively Impacted Business Finances
(Shown % Select , among those who have experienced a cyberattack)



Nationwide®

*Q11B. What was the financial impact of the cyberattack on your company? If your company has experienced more than one attack in the past three years, please refer to the **most recent** attack.*
Q11C. Did the cyberattack interrupt your company's usual business and operations? Base: Risk Manager who have experienced a cyberattack in past 3 years (Total: n=340)

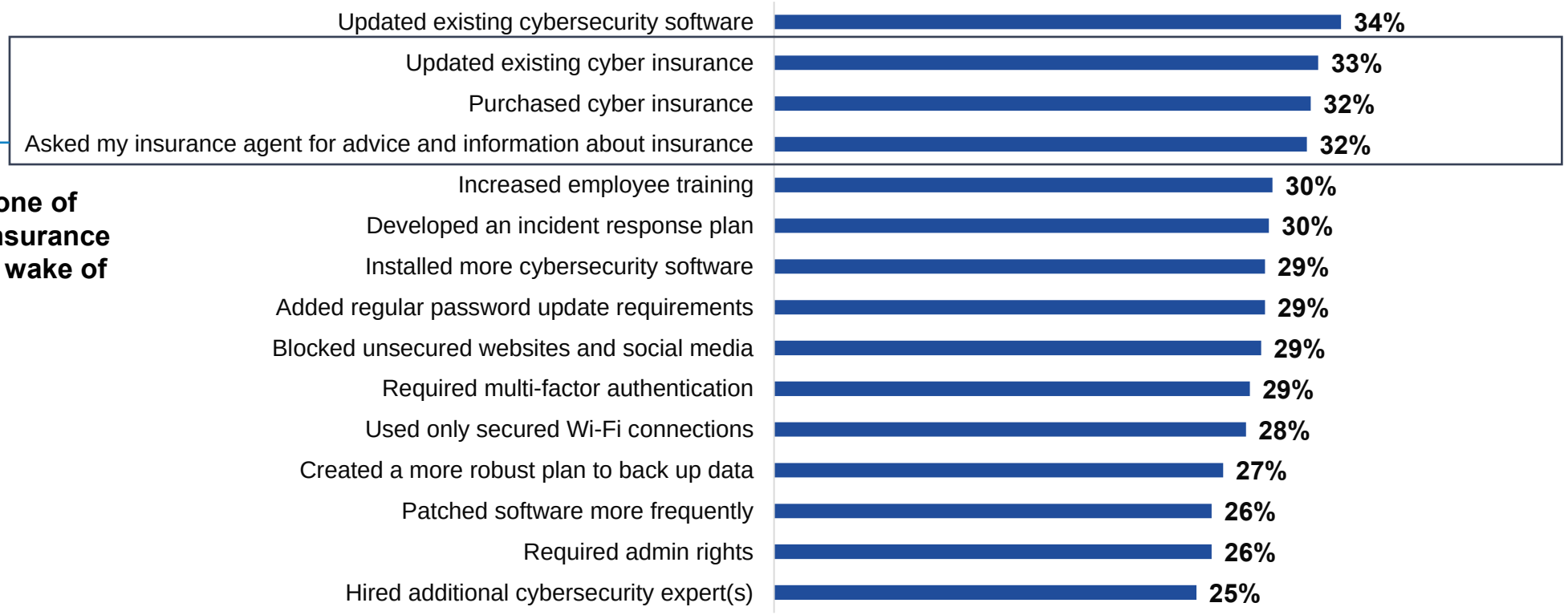
Almost 8 in 10 risk managers updated, purchased, or sought more information about cyber insurance after their employer experienced a cyberattack

77%

Took at least one of these cyber insurance actions in the wake of the attack

Cybersecurity Measures Implemented After Attack

(Shown % Select, among those who have experienced a cyberattack)



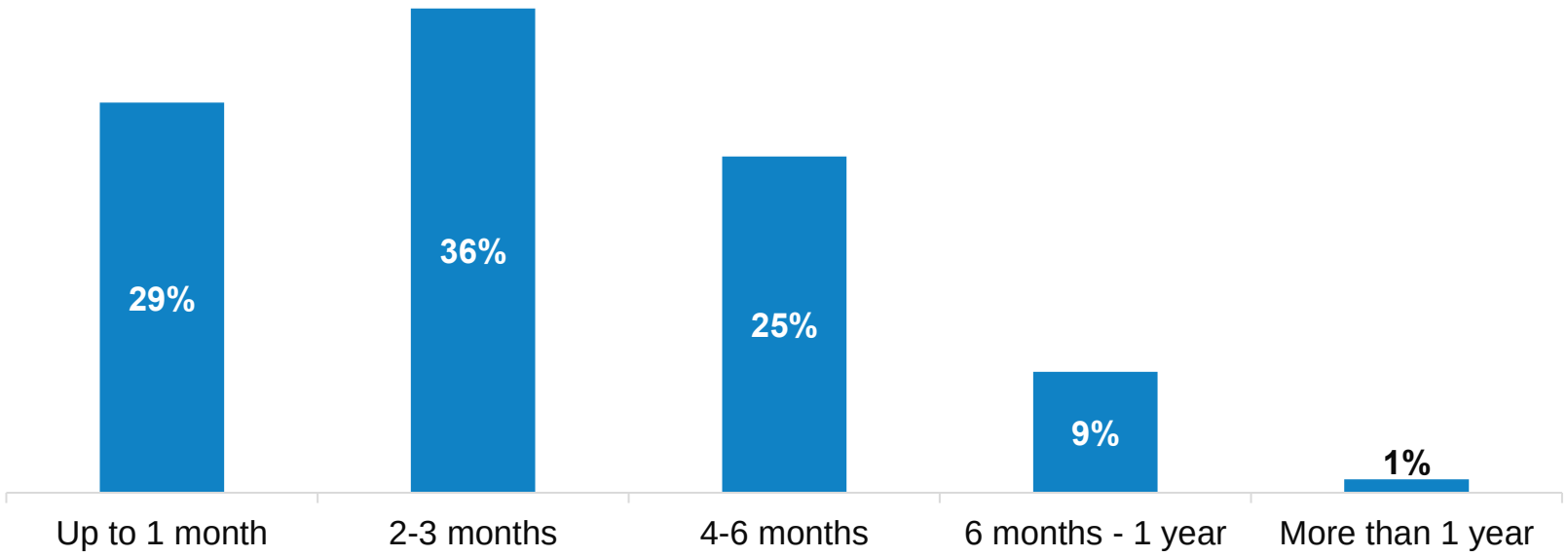
Nationwide®

Q11E. What additional cybersecurity measures has your company implemented since experiencing the attack? Please select all that apply.
Base: Risk Managers who have experienced a cyberattack (Total: n=438)

Most risk managers who have experienced a cyberattack say the recovery process took several months

Length of Time to Recover From a Cyber Attack

(Shown % Select , among those who have experienced a cyberattack)



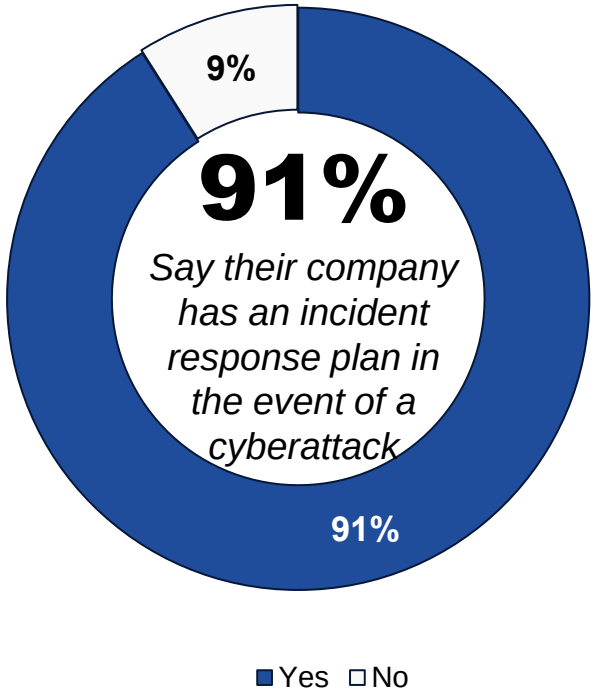
Nationwide®

Q11D. About how long did it take your company to recover from the cyberattack? Base: Risk Managers who have experienced a cyberattack in past 3 years (Total: n=340)

Though concern about cyber threats is high, nearly all risk managers feel their employer is prepared to recover from future attacks

Preparedness for Recovering from a Cyberattack
(Shown % Select)

Incident Response Plans
(Shown % Select 'Yes')



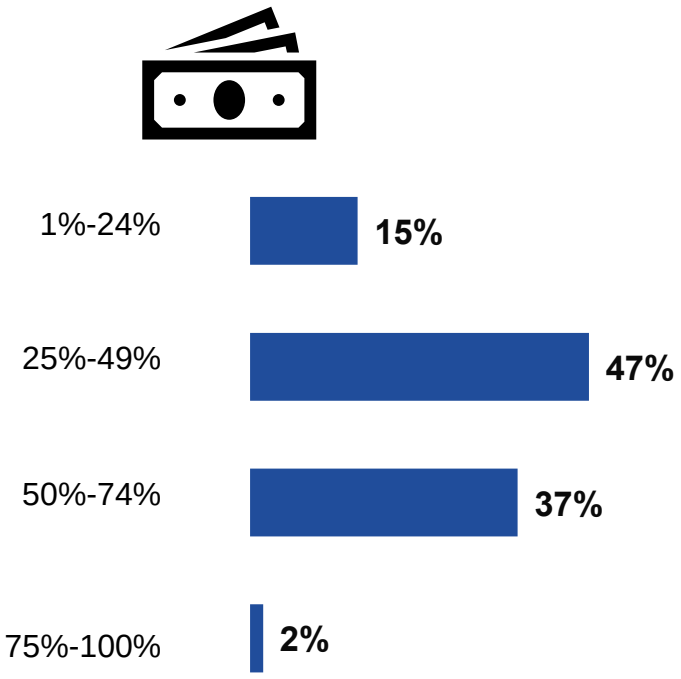
Nationwide®

Q6. How prepared do you think your company is to recover from a cyberattack? Base: Risk Manager (Total: n=500)
Q7. Does your company have an incident response plan in the event of a cyberattack? Base: Risk Manager (Total: n=500)

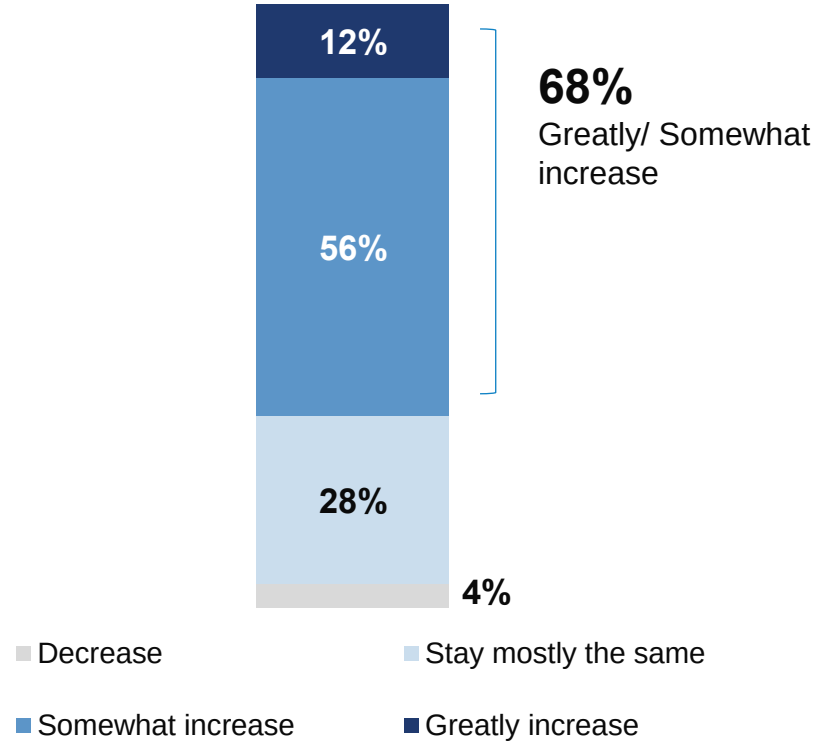
Cyber Insurance

Cybersecurity takes up a substantial portion of IT budgets, and risk managers expect these budgets will continue to grow in the coming years

Current Percent of IT Budget Dedicated to Cybersecurity
(Shown % Select)



Expected Change in Cybersecurity Budget Over Next Three Years
(Shown % Select)

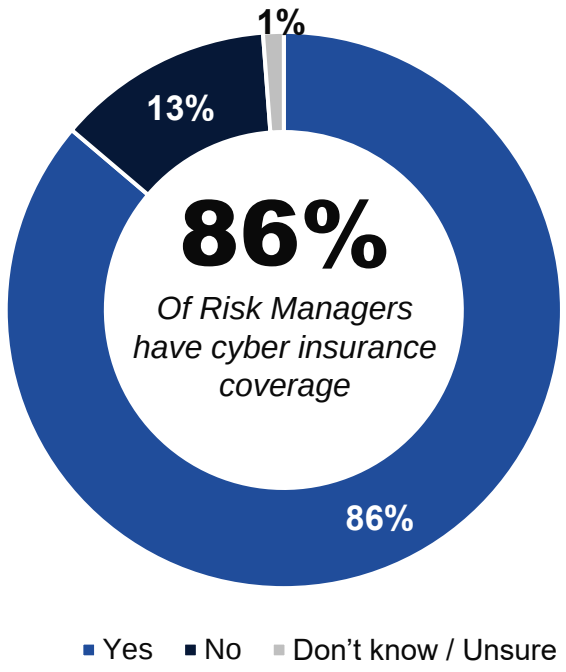


Nationwide®

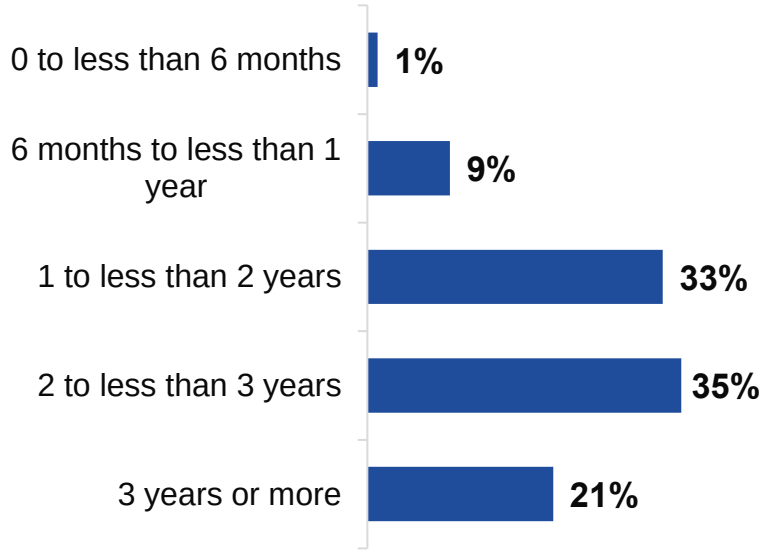
Q18. To the best of your knowledge about what percent of your company's total IT budget is dedicated to cybersecurity, including cyber insurance and any third-party vendors?
Q19. Looking ahead to the next three years, how do you expect your company's budget for cybersecurity and cyber risk management will change? Base: Risk Manager (Total: n=500)

Cyber insurance has been almost universally adopted, with most companies carrying a policy for several years

Employer Cyber Insurance Coverage
(Shown % Select)



How Long Employer Has Had Coverage
(Shown % Select, among those who have cyber insurance)

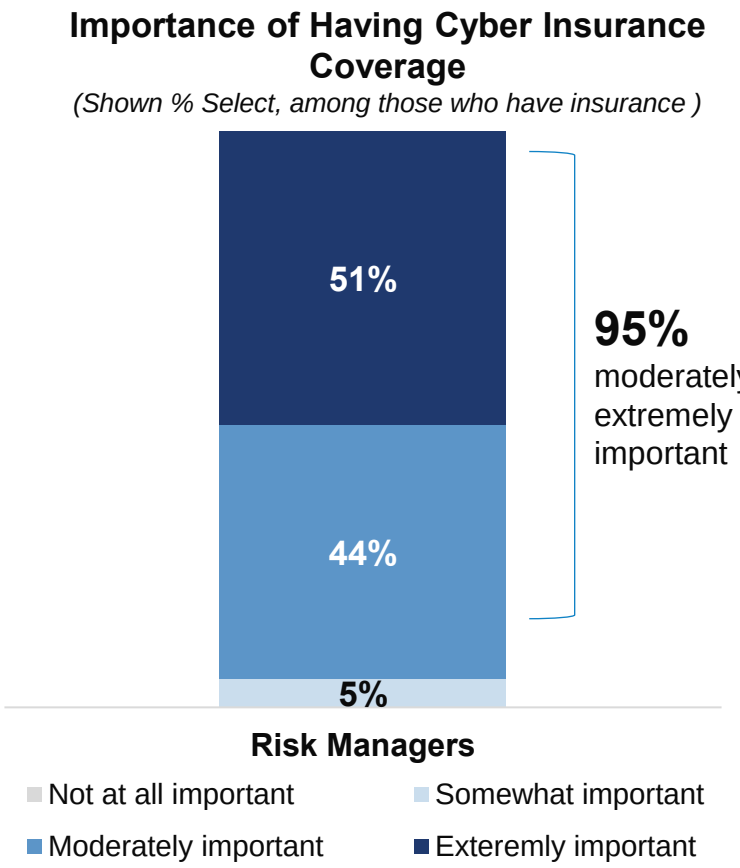


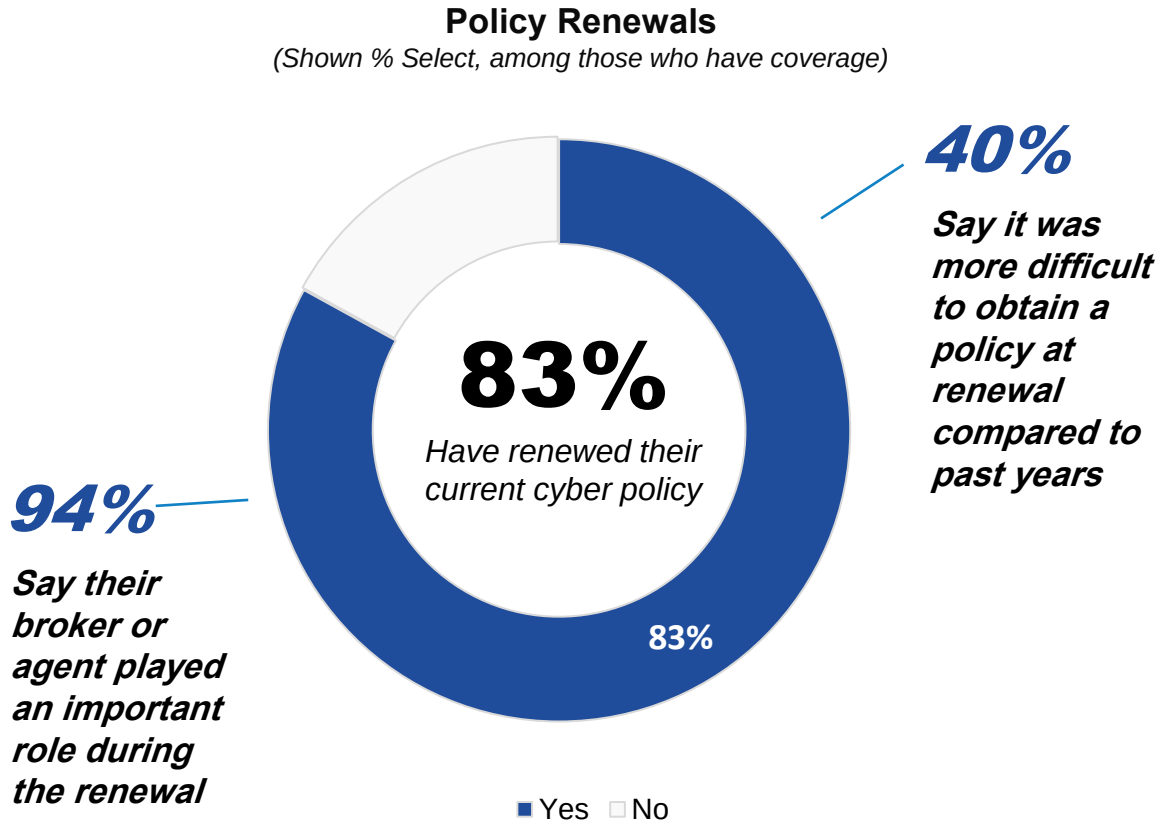
Nationwide®

Q16. Does your company purchase cyber insurance? Base: Risk Manager (Total: n=500)
Q16A. How long has your company had cyber insurance coverage? Base: Risk Managers who have insurance (Total: n=431)

Risk managers see cyber insurance as a critical element of security policy

More than 8 in 10 have renewed their current policy.





Nationwide®

Q16D. Has your company renewed its cyber insurance policy? Base: Risk Managers who have insurance (Total: n=431)
Q16J. How important do you think it is for your company to have cyber insurance coverage? Base: Risk Managers who have insurance (Total: n=431)
Q16E. Did your cyber insurance agent or broker play an important role at the last renewal? Base: Risk Managers who have renewed cyber insurance policy (Total: n=358)
Q16F. Was is more difficult to obtain a policy at last renewal? Base: Risk Managers who have renewed cyber insurance policy (Total: n=358)

Risk Managers work closely with the C-Suite when making decisions about cyber coverage, and 9 in 10 are comfortable understanding their policy

Cyber Insurance Policy
(Shown % Top 2 Box)

94%

Worked closely with their CISOs or other head of cybersecurity to obtain cyber insurance coverage.

- Very closely
- Somewhat closely
- Not too closely
- The CISO / head of cybersecurity was not involved

90%

Indicated they are **comfortable understanding** what their company's cyber insurance policy covers.

- Very comfortable
- Moderately comfortable
- Somewhat comfortable
- Not at all comfortable

Nationwide®

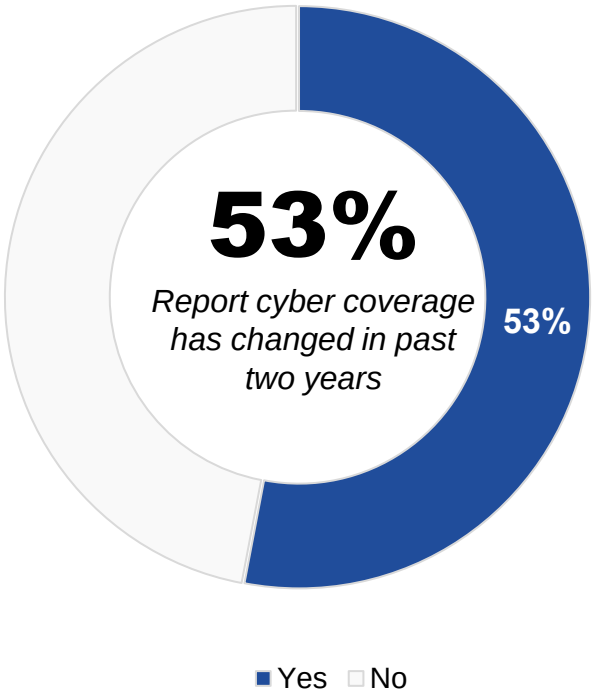
Q16B. How closely did you (or other staff members responsible for risk management) work with your company's Chief Information Security Officer (CISO) or other head of cybersecurity to obtain cyber insurance coverage? Q16C. How comfortable are you understanding what your company's cyber insurance policy covers? Base: Risk Manager who have insurance (Total: n=431)

Half have recently changed some element of their cyber coverage, but the reasons for changes vary

Insurance carriers changing terms, inability to get the desired limit, and bad claim experiences are some of the most common reasons cited.

Coverage Recently Changed

(Shown % Select, among those who have insurance)



Reasons for Changing Cyber Insurance Coverage

(Shown % Select, among those who have changed their coverage)

1	Insurance carrier changed their terms	**37%**
2	Could not get the limit we wanted	**36%**
3	Bad claim experiences	**36%**
4	Our company's risk profile impacted coverages we could get	**35%**
5	Did not fully understand what was covered	**34%**
6	Insurance carrier was difficult to work with	**34%**
7	Our business operations / needs have changed	**32%**
8	Our previous agent left or retired	**28%**
9	The coverage was too expensive at renewal	**27%**

Q16G. Has your company's cyber insurance coverage changed in the past year or two? Base: Risk Managers who have insurance (Total: n=431)
Q16I. Why did your company change its cyber insurance coverage? Please select all that apply. Base: Risk Managers who have changed their coverage (Total: n=229)

When making cyber policy changes, most risk managers look to increase their coverage and retention, and buy more limit

How Cyber Insurance Policy Has Changed

(Shown % Select, among those who changed their policy)

Q16H. In what ways has your cyber insurance coverage changed in the past year or two? Base: Risk Managers whose cyber insurance coverage has changed (Total: n=229)