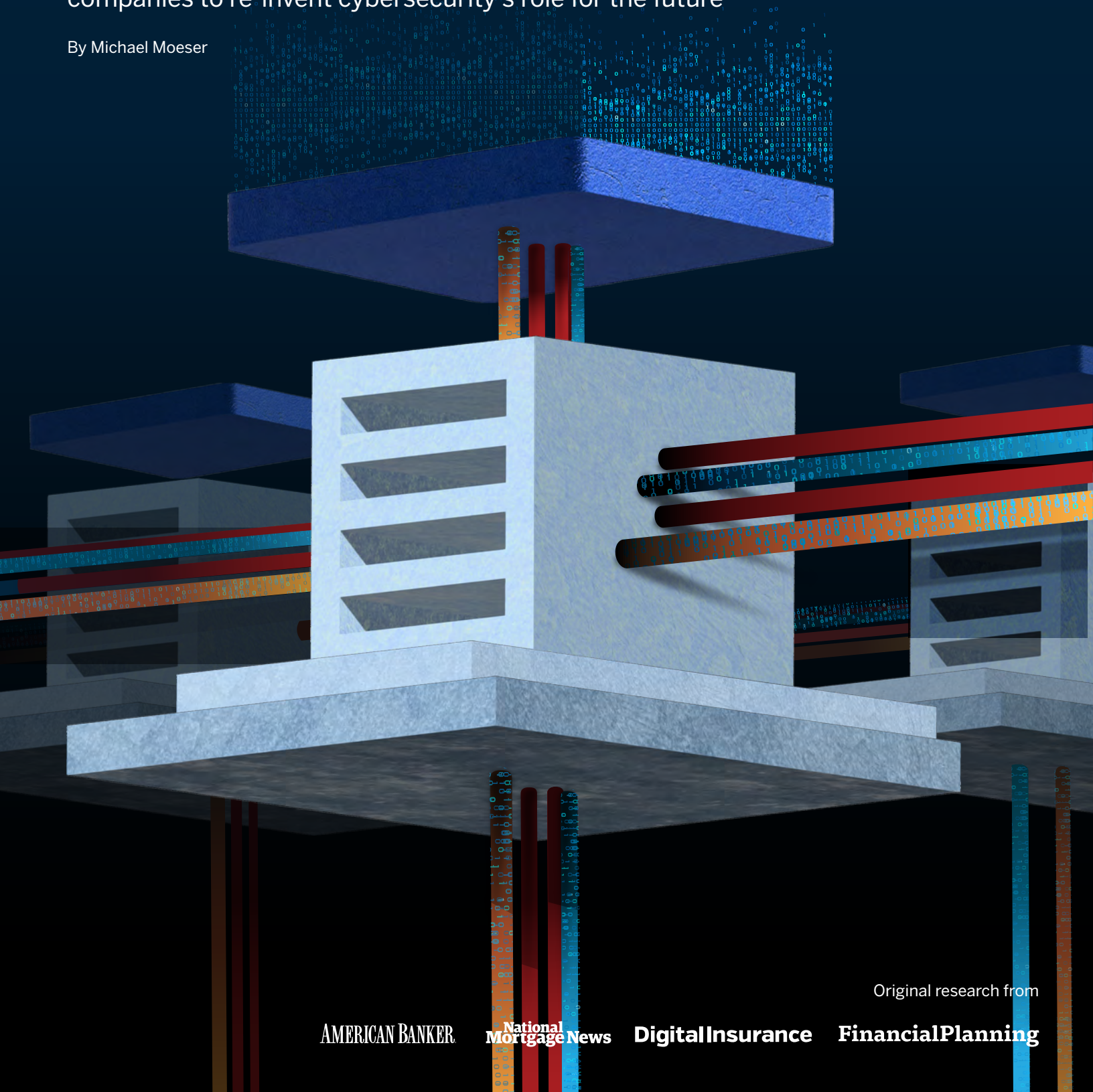
STATE OF CYBERSECURITY 2022

Enabling Innovation: Cybersecurity's Next Act

Changing consumer expectations, new workplace realities and increasing demand for third-party access to data are pushing companies to re-invent cybersecurity's role for the future

By Michael Moeser



Original research from

American Banker | National Mortgage News | Digital Insurance | Financial Planning

Enabling Innovation: Cybersecurity's Next Act

Introduction

The state of cybersecurity is going through a metamorphosis as financial services leaders prepare their organizations for the future. Leaders are transitioning from a mentality of fortifying the IT perimeter to one where an organization provides secure, distributed access to customers, staff and third-parties. The rise of the mobile channel, growing demand for third-party access to customer data, new vendors being deployed for product innovation and remote workforces are just a few of the examples of what is driving this shift.

Yet none of these phenomena are completely new. Many have been occurring in the background for some time, such as the growing importance of the digital channel, while others became more widespread in the last two years, such as employees working from home. Furthermore, there were certain third-party consumer-directed services that traditionally catered to younger consumers that are now reaching a broader audience, such as P2P money transfers, that have made providing secure data access to a third-party a priority for many financial institutions.

The accelerant behind these changes was the COVID-19 pandemic and the effects that the virus has had on how businesses operate and how consumers engage with them appear to be longer lasting. That is, once the pandemic fades into the history books, many of the changes brought on by the impact of the virus are likely to remain and grow in popularity due to the convenience and greater access they offer, such as employees working remotely, consumers digitally acquiring and servicing financial products and the use of mobile wallets.

Unfortunately, as managing access to identities, data and devices has increased in complexity, cybercrime has also grown. This has pushed up cybersecurity defenses that can inadvertently act as a roadblock to innovation and product development, underscoring the importance of having the right strategy to enable business transformation.

This report explores the current state of cybersecurity, the way leaders across financial services are working to protect and provide access to their data and the impact breaches have had in how organizations approach cybersecurity.

Why read this report?
This report provides insights into the cybersecurity strategies and priorities across the banking, insurance and wealth management industries. It specifically reviews how companies are testing their vulnerabilities as well as mitigating the growing risks as consumers shift to digital channels.

Key findings

- There is high confidence that companies are taking the necessary steps on cybersecurity to establish or maintain a best-in-class position among core competitors, particularly among banking and insurance leaders. This is notable since banking and insurance companies report twice the breach rate compared to wealth management firms.

- Getting breached has a two-fold effect on a company's top cybersecurity priorities: 1) breached companies report a wider set of top priorities vs. unbreached firms, who tend to focus primarily on keeping up-to-date on threats; and 2) breached companies value cybersecurity staff training as highly as keeping up-to-date on threats. This underscores the fact that monitoring threats is valuable only if your organization is not an early victim of a trend, whereas training becomes invaluable to a threat response.

- There is no single factor contributing to the growing cybersecurity risk profile of the companies surveyed. Rather, there is a collection of factors that points to a common theme of increasing data access needs. Four factors affect 40% or more of the respondents' organizations: 1) customers using mobile devices to access their data while "on the go"; 2) employees working remotely; 3) new digital tools being used to access customer data; and 4) third-parties being directed by customers to access their data.

- Respondents are aware of the growing data access demands by customer-directed third-party apps and expect that this trend will require new policies and processes, changes in identity management practices and new customer validation procedures.

- One out of three organizations acknowledges the struggles they face in trying to balance the need for more robust cybersecurity with innovation and product development goals.

- The biggest threats leaders expect in the next 12 to 24 months are viruses and malware, followed by data breaches and then phishing/spear phishing. Additionally, leaders have a multitude of concerns weighing on their minds, beginning with identifying and preventing fraudulent activity, followed by data privacy compliance and email security.

- Three out of four respondents expect their organization's overall cybersecurity spending to increase year-over-year, with more than half (58%) reporting a 10% or more increase. More than half of all respondents already use cybersecurity risk liability insurance, with more than one-quarter planning to purchase it in the next 12 months.

- Two-factor authentication is the top strategy being implemented to serve customers, employees and third-party vendors more safely, followed by device registration.

- There is no single approach to assessing an organization's cybersecurity vulnerability, as many use some of the same approaches with two exceptions—the banking sector is a far stronger user of attempting to hack into its own systems and practices periodic data breach simulations.

About this report

Arizent, publisher of leading brands in financial services including American Banker, The Bond Buyer, Financial Planning, National Mortgage News and in professional services, such as Accounting Today, Employee Benefit News and Digital Insurance conducted this survey to explore the current state of cybersecurity, how organizations are adapting to the changing business environment and what future plans companies are considering implementing.

The survey was conducted online between November 24 and December 28, 2021 with 192 U.S. business leaders in three specific areas: 1) banking, including mortgage and payments divisions (51% of respondents); 2) wealth management (28%); and 3) insurance carriers (21%). One-third (33%) of respondents are at the C-suite level and 56% of overall respondents are employed in an IT or IT security function.

Approximately 37% of respondents work in organizations with 1,000+ employees, 34% with 100-999 employees and the remainder in firms with fewer than 100 employees. Approximately 83% of banking and 90% of insurance carriers have more than 100 employees, and 44% and 56%, respectively, have more than 1,000 employees. Wealth management firms surveyed are smaller, with 64% having fewer than 100 employees, 28% having between 100-999 employees and 8% having more than 1,000 employees.

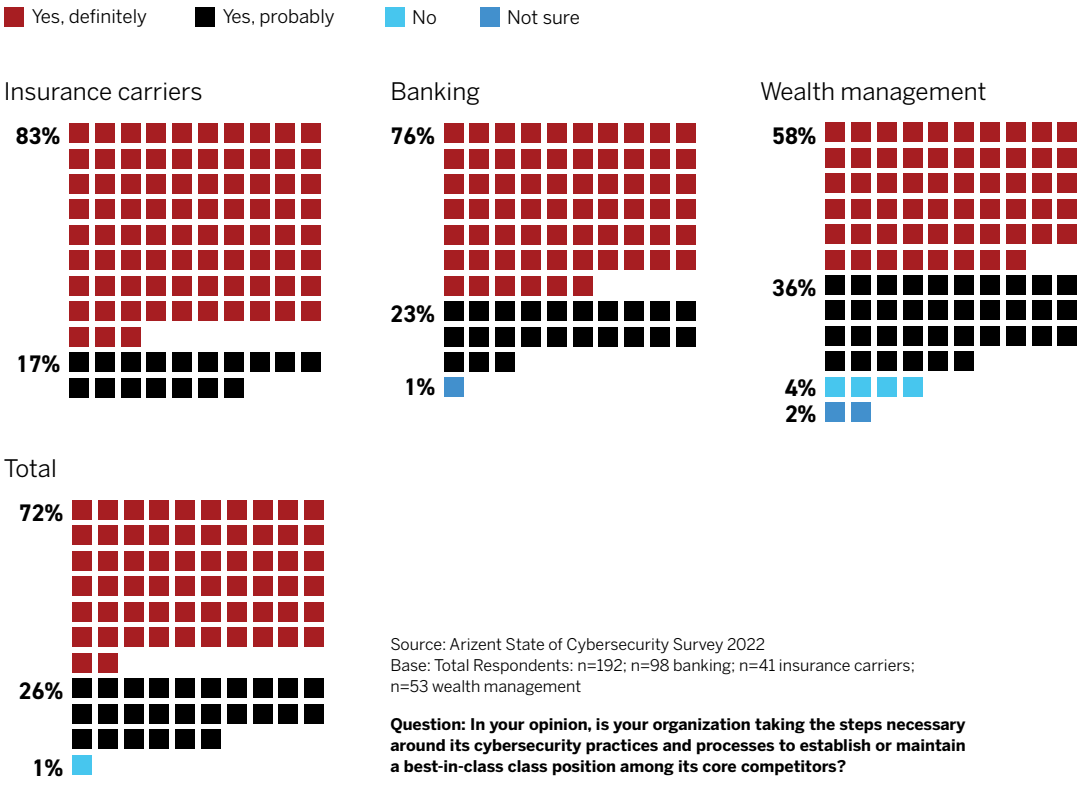
Confidence is high in how cybersecurity is being handled

Respondents are confident that their companies are taking the steps needed on cybersecurity to establish or maintain a best-in-class position among core competitors within financial services. Insurance carrier business leaders are the most confident, with 83% reporting that their organizations are "Yes, Definitely" taking the needed steps, followed by banking leaders at 76% (see Figure 1). Confidence levels among wealth management leaders are high, albeit not as strong as the other two financial services sectors.

One possible factor behind the statistical difference in confidence levels may be the fact that the wealth management organizations surveyed are significantly smaller, with 64% having fewer than 100 employees compared to just 17% of banks and 10% of insurance carriers. Among the larger organizations overall, with 1,000+ employees, which includes the largest wealth management firms surveyed, 84% of leaders report a "Yes, Definitely" high confidence level in their cybersecurity approaches. In essence, a larger organization with more employees will generally support bigger IT budgets and more staff to approach cybersecurity with the latest tools and processes. Nonetheless, it should be noted that only 4% of wealth management business leaders report a vote of "No" confidence in their cybersecurity strategies.

Figure 1: Banking and insurance are the most confident in their cybersecurity strategies

Confidence level organization is taking the necessary steps to establish/maintain best-in-class position



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management

Question: In your opinion, is your organization taking the steps necessary around its cybersecurity practices and processes to establish or maintain a best-in-class class position among its core competitors?

At **94%**, early adopters of new technology are the most confident that they are "yes, definitely" taking the needed steps to best manage cybersecurity.

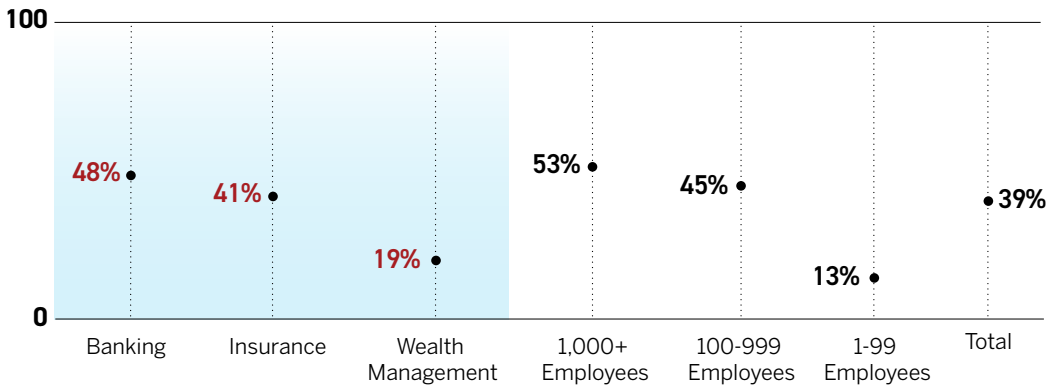
One additional finding is that business leaders from companies which have suffered a data breach in the last five years report a higher level of confidence in their approach to cybersecurity for establishing or maintaining a best-in-class position relative to their competitors. Among those who have suffered a breach, 82% answer "Yes, Definitely" to this question compared to 66% of business leaders from companies that have not suffered a breach. It is very likely that the experience of having suffered a breach has caused these leaders and their companies to review policies and procedures regularly to establish and maintain a top performing cybersecurity approach.

Understanding data breaches provides insights on cybersecurity defenses and priorities. Having a system breached is a major loss event and weighs heavily on cybersecurity policies and practices. Certain sectors have experienced higher levels of breaches due to a combination of their attractiveness to criminals—large financial databases with customer information, rapid money transfer capabilities, etc.—and the size of their organization—big companies make for big targets. Banking and the insurance industries have experienced the highest levels of data breaches in the past five years among those surveyed at 48% and 41%, respectively, compared to only 19% of wealth management firms (see Figure 2).

The size of an organization, based on number of employees, is also a factor in data breaches, with larger companies having a higher likelihood of being exposed to a hack than smaller companies—53% of companies surveyed with 1,000+ employees have experienced a breach compared to 45% of companies with 100-999 employees and 13% of companies with fewer than 100 employees.

Figure 2: Banking, insurance and larger organizations are more likely to have suffered a breach

Percent (%) who have experienced a data breach in past five years



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management; n=70 1,000+ employees; n=67 100-999 employees; n=55 1-99 employees

Question: In the last five years, has your organization suffered a data breach where an unauthorized individual or group gained access to customer data, employee data, financial transactions, payment details and other sensitive information?

The factors contributing to a data breach are more varied among banking and insurance companies, which in turn means that there is no single threat to defend against. For example, insurance respondents report seven different factors contributing to at least one-third of breaches experienced.

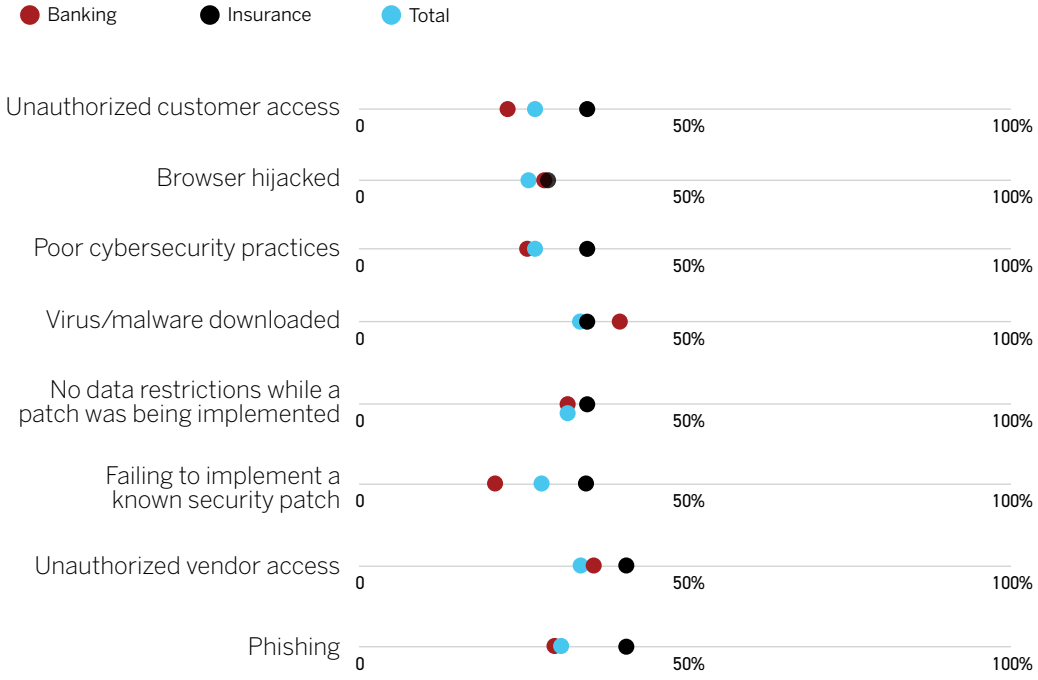
Among the banking respondents, virus download is the top contributing factor to data breaches at 40%, followed by unauthorized vendor access (36%), no data restrictions while a security patch was being implemented (32%) and phishing attempts (30%). For the insurance industry, the top two factors are tied at 41% each—phishing and unauthorized vendor access (see Figure 3). The next five contributing factors are cited by 35% of insurance respondents.

The impact of a breach seems to have a two-fold effect on a company's cybersecurity priorities. First, breached companies report a wider set of top priorities, unlike those that have not been breached which focus primarily on keeping up-to-date on cybersecurity threats at 73%. Second, breached companies value cybersecurity staff training (61%) as highly as they do keeping up-to-date on threats (57%). The logic is that watching out for trends is valuable only if your organization is not an early victim in a trend, because that's where staff training becomes critical in responding to the threat.

"We need to establish a Cybersecurity agency to research and coordinate efforts to lessen cybersecurity risks," President, Asset Management Firm.

Figure 3: There is no single factor to defend against that can prevent most breaches

Factors most often contributing to data breaches



Source: Arizent State of Cybersecurity Survey 2022
Base: Respondents n=98 banking; n=41 insurance carriers

Question: Which of the following factors contributed to the data breach?

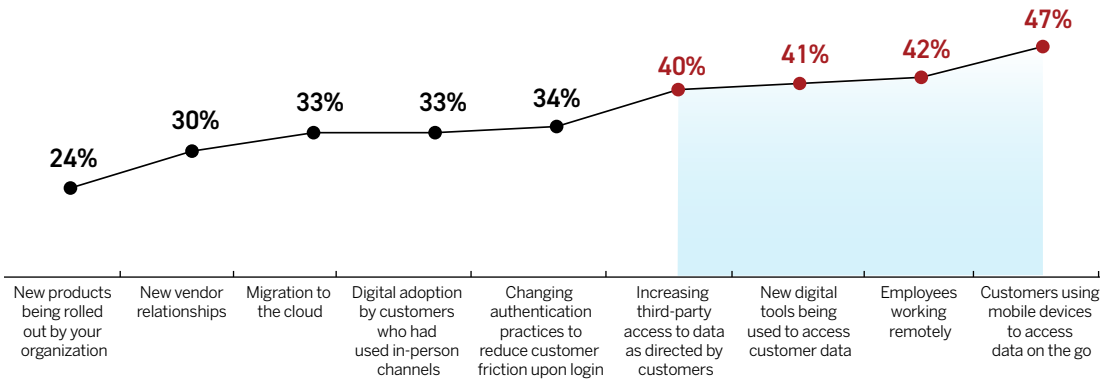
Cybersecurity risks are growing as data access demand and faster money usage expand

There is no single factor contributing to the growing cybersecurity risk profile of the companies surveyed. Rather, there is a collection of factors that points to a common theme of increasing data access to customers, third-parties and employees working remotely or from home. In fact, four factors affect 40% or more of the respondents' organizations: 1) customers using mobile devices to access their data while "on the go" at 47%; 2) employees working remotely at 42%; 3) new digital tools being used to access customer data at 41%; and 4) third-parties being directed by customers to access their data at 40% (see Figure 4).

While a number of these factors had been present prior to the pandemic, office and branch closures have had a more immediate impact in accelerating the need for data access by an institution's customers and employees. There is a strong likelihood that as the pandemic subsides many of these factors will continue to be impactful, as many companies consider providing permanent worker flexibility and consumers continue to migrate to digital channels.

Along with greater data access demands, the growing adoption of faster money movement in transfers and bill payments is also a factor in raising cybersecurity risk profiles for about 65% of banks, 55% of wealth management firms and 54% of insurance carriers.

Figure 4: Greater data access is raising cybersecurity risk profiles
Factors increasing an organization's cybersecurity risk profile



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192

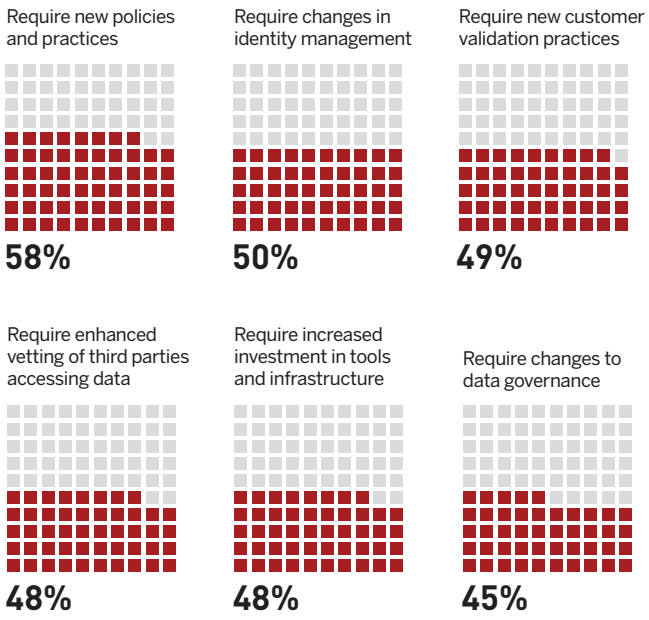
Question: What factors do you think are increasing your organization's cybersecurity risk profile?

Business leaders are keenly aware of the growing demands by customer-directed third-party applications seeking access to their data. Anytime a consumer uses an online tax service, e.g., H&R Block, a personal financial management app, e.g., Intuit's Mint, or a digital mortgage provider, e.g., Rocket Mortgage, the third-party reaches out to a financial services company for access to the customer's own data. The challenge then becomes how to safely provide access and manage the process.

Financial leaders expect that the rise in third-party data access will require them to adapt to this ever-expanding access point. More than half (58%) state that third-party data access will require new policies and practices to manage these third-party encounters (see Figure 5). About half (50%) expect it will require changes in identity management practices and 49% state it will require new customer validation procedures.

Figure 5: Business leaders expect increased third-party data access will require them to adapt

Cybersecurity impacts due to greater third-party access to data



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192

Question: What impacts will providing greater third-party access to your customers' data as requested by your customers, e.g., open banking, financial aggregators, wealth management apps, insurance aggregators, have on your cybersecurity infrastructure?

fanniemae.com/research-and-insights/perspectives/pandemics-impact-mortgage-digitization-and-homebuyer-satisfaction

Fannie Mae reports that 41% of first-time home buyers allow third-party access to their financial data for mortgage origination, compared to 33% of repeat home buyers.

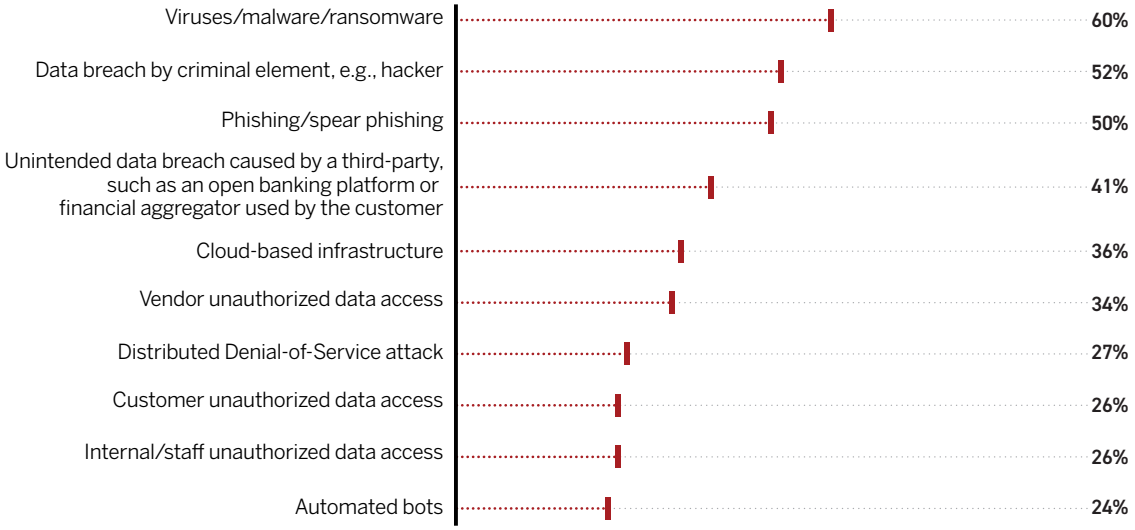
Future cybersecurity threats weigh heavily on leaders' minds

Despite data breaches being so impactful on an organization, it's not the biggest cybersecurity threat respondents expect in the next 12 to 24 months—it's viruses, malware and ransomware at 60% of respondents (see Figure 6). Data breaches are the second biggest risk to leaders at 52%, followed by phishing/spear phishing at 50%. While viruses and malware can often lead to data breaches, they don't always, as attackers can have an ulterior motive, such as shutting down new credit card applications or causing an outage in an online account management server, among other things.

Additionally, mortgage business leaders were asked a separate question about which areas are of greatest concern to them regarding future fraudulent activity. Here, there is a tie at 65%, with the top two responses being income and employment fraud, and undisclosed real estate debt. Wire fraud at mortgage closing is the third biggest fraud concern at 55%, followed by occupancy fraud at 50%, identity fraud at 40% and in last place property valuation fraud at 30%.

Figure 6: Business leaders see viruses as the biggest threat in the near future

Greatest cybersecurity risks expected over the next 12 to 24 months



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192

Question: What types of attacks do you think pose the greatest risk to your business over the next 12 to 24 months?

Beyond operational priorities and future threats, respondents have a multitude of cybersecurity concerns that they must contend with on a daily basis, which is stretching their resources thin and impacting a number of different functional units beyond the IT department, such as fraud, risk, compliance, underwriting, product management and more.

The top cybersecurity concern weighing on business leaders' minds is identifying and preventing fraudulent activity at 41%, followed by data privacy compliance at 40% and email security at 38% (see Figure 7). Since many viruses are often downloaded by fraudulent or tampered emails, it should come as no surprise that email security is a top-three cybersecurity concern. Furthermore, there are a total of 11 other top concerns that hold at least a 25% share among respondents, demonstrating how complex and arduous a challenge cybersecurity is for an organization to manage.

Figure 7: Other top concerns include identifying/preventing fraudulent activity

Other cybersecurity concerns that are top of mind

Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192

Question: What other cybersecurity concerns are top of mind for your organization?

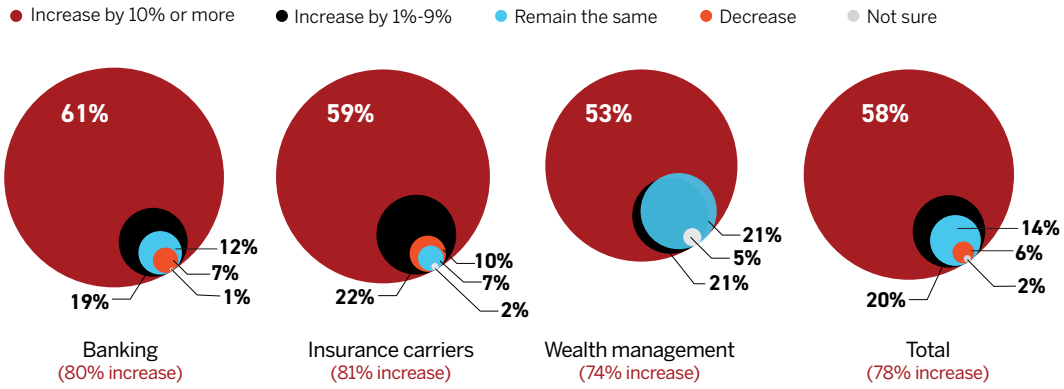
Email security is a greater concern among wealth managment firms at 49% compared to banks at 37% and insurance carriers at 27%.

Increased resourcing and risk insurance are the cavalry for many

Due to a more challenging cybersecurity environment, three out of four (78%) respondents across financial services expect their organization's overall cybersecurity spending to increase year-over-year, with more than half (58%) reporting a 10% or more increase (see Figure 8). The increase levels are relatively even across all three sectors, ranging from 81% of insurance carriers to 74% of wealth management expecting an increase. Very few expect their budgets to remain the same and fewer than than 10% overall expect them to decrease.

Figure 8: Three quarters expect their budgets to increase

Expected cybersecurity funding changes in next 12 months



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management

Question: In the next 12 months, how do you expect your organization's overall cybersecurity spend (on capital expense, operational expenditures, people and other resources) to change compared to the previous 12 months?

In response to the growing financial losses cybersecurity threats can pose, more than half (54%) of all respondents already use cybersecurity risk liability insurance, with more than one-quarter (29%) planning to purchase it in the next 12 months and just under a tenth (9%) considering it, but having no firm purchase plans. Insurance carriers are the highest current users of risk liability insurance at 63%, followed by banking at 54% and then wealth management at 45%. In terms of planning to purchase insurance in the next 12 months, banking is top with 34%, followed by insurance at 29% and wealth management at 19%.

Given the prevailing attitudes toward purchasing cybersecurity risk liability insurance, it is very likely that in the near future it may become a de facto standard among financial services organizations. While this type of insurance is not required, unlike for instance how FDIC deposit insurance is required for banks, it will become "the" prudent decision for companies. It would be similar to public companies purchasing director and officer (D&O) insurance to protect their board of directors from personal losses if they are sued as a result of serving on the board. Without D&O insurance, it would be nearly impossible to recruit directors for a public company.

Two-factor authentication comes to the rescue

Balancing the need for stronger cybersecurity defenses with product development and innovation goals is a challenge for many financial services organizations. In fact, about one-third (35%) of survey respondents report that the need for strong cybersecurity has a negative impact on innovation and product development at their organizations. Banks feel this most keenly at 41%, followed by insurance carriers at 37% and then wealth management firms at 23%. This challenge demonstrates the need to have a well-balanced and comprehensive cybersecurity strategy to help the business transform for the future.

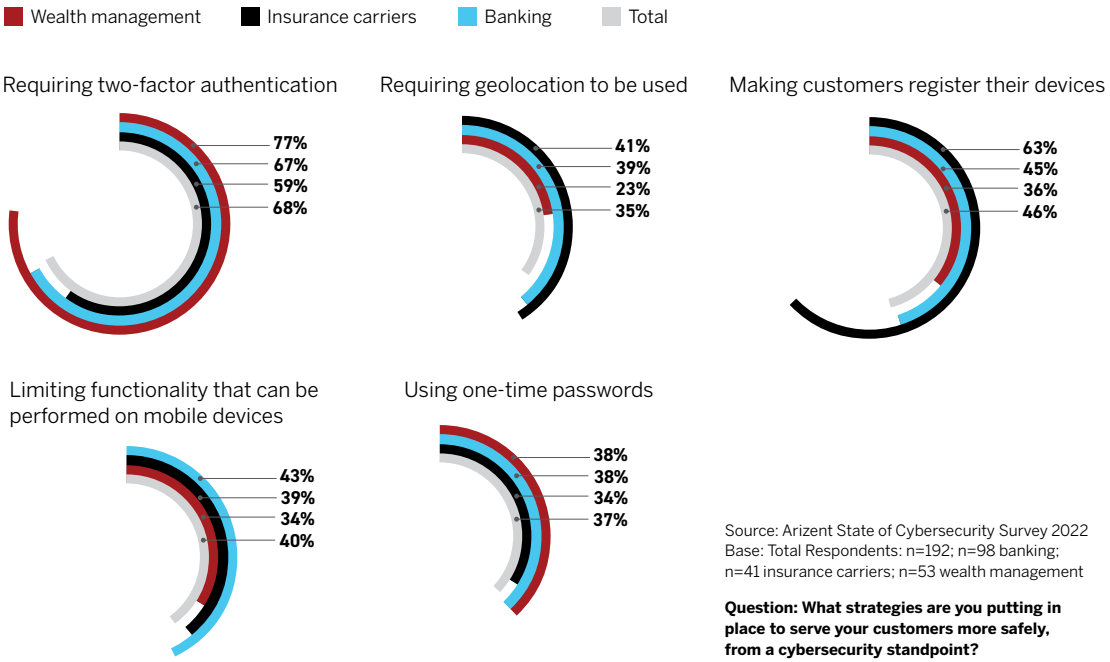
When it comes to strategies being deployed to serve their customers more safely, a majority of financial leaders (68%) report they are implementing two-factor authentication, followed by making customers register their own devices at 46% (see Figure 9). Two-factor authentication usage is the highest among wealth management at 77% and the lowest among insurance carriers at 59%, with banking in the middle at 67%.

Older methods such as one-time passwords (OTP) are not as popular, nor is requiring the use of geolocation. The OTP strategy has known security limitations, while geolocation is a more complex issue because it involves customer privacy and compliance. Although limiting the functionality that can be performed on mobile devices is being used by at least a third of organizations, it poses a customer experience challenge as the mobile channel grows, introducing friction for the customer and increasing the risk of customer attrition.

Companies increasing their cybersecurity budgets by 25% or more had the most favorable view of two-factor authentication with 81% deploying it for customers.

Figure 9: Two-factor authentication is the leading customer-facing cybersecurity strategy

Strategies being put in place to serve customers more safely, from a cybersecurity standpoint



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management

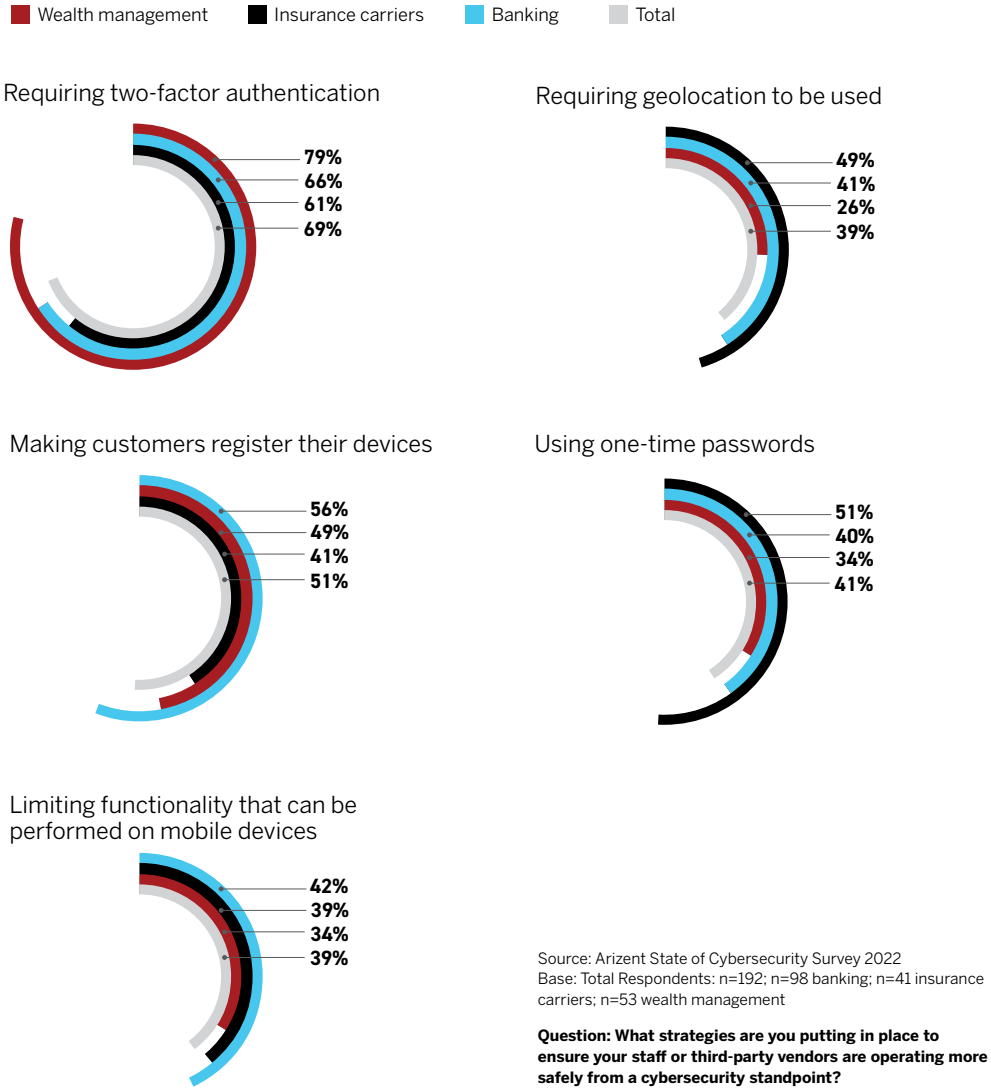
Question: What strategies are you putting in place to serve your customers more safely, from a cybersecurity standpoint?

In the same vein, leaders are putting their resources into deploying two-factor authentication as a key strategy to serve their employees and third-party vendors more safely at 69% overall, followed by device registration at 51%, using OTPs at 41%, and geolocation and limiting mobile device functionality at 39% each (see Figure 10).

There are some notable differences within certain financial sectors in treating the different populations. In the insurance sector, device registration (63%) is the top strategy to serve customers more safely followed by two-factor authentication (59%). However, when it comes to employees and vendors, two-factor authentication is the leading strategy at 61%, but device registration is second to last at 41%.

Figure 10: Two-factor authentication is the leading employee/vendor-facing cybersecurity strategy

Strategies being put in place to ensure employees or third-party vendors are operating more safely



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management

Question: What strategies are you putting in place to ensure your staff or third-party vendors are operating more safely from a cybersecurity standpoint?

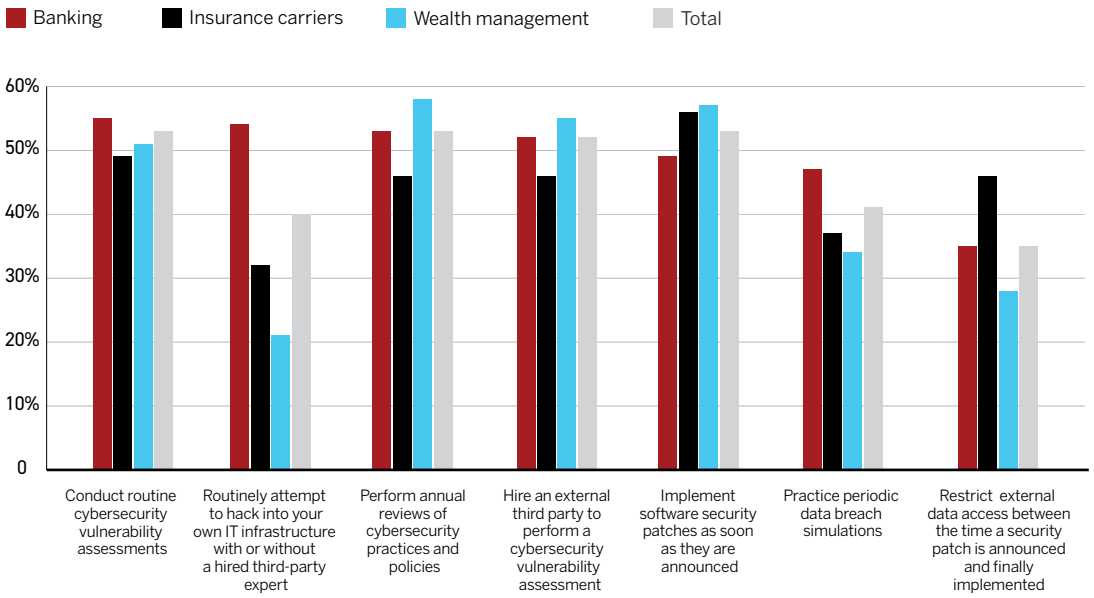
Companies are just at the tipping point for proactively looking for vulnerabilities

There is no single "silver bullet' approach to assessing an organization's cybersecurity risk vulnerability, as many use some of the same approaches with two exceptions—the banking sector is a far stronger user of attempting to hack into its own systems with or without a third-party involved at 54% and practices periodic data breach simulations at 47% (see Figure 11).

Unfortunately, while almost all organizations conduct annual performance reviews of their employees, only half conduct annual performance reviews of their cybersecurity practices and policies. These are valuable tools that can inform investment decisions and identify where resources need to be added or reduced.

Figure 11: Half of banks hack into their systems to test their vulnerability

Steps used to assess and address cybersecurity vulnerabilities



Source: Arizent State of Cybersecurity Survey 2022
Base: Total Respondents: n=192; n=98 banking; n=41 insurance carriers; n=53 wealth management

Question: What steps is your organization taking in assessing and addressing its cybersecurity vulnerability?

Conclusions

- Contrary to expectations, the future of cybersecurity is to open a financial institution's access to its customers and data to enable growth. Executive mindsets need to shift away from the perception of cybersecurity as a closed fortress to protect the institution's data, systems and tools. Instead, providing secure, distributed access to data, systems and tools will enable an institution to be flexible and agile enough to capitalize on opportunities and respond to challenges.

- There is widespread acknowledgement that the need to provide greater third-party access to customer data will require changes in many areas. Therefore, financial institutions must immediately start understanding how their organizations will need to adapt, what resources will be required to implement changes and how they can build flexibility into their systems as demand and competitive pressures to provide data access grow.

- Institutions need to re-prioritize their top operational concerns, particularly those who believe keeping up-to-date on cybersecurity threats should be their primary focus. Breached companies provide valuable insights, as they value cybersecurity staff training equally with keeping up-to-date on threats, very closely followed by finding the right solutions/partners. Hyper-focusing on monitoring threats leaves an organization vulnerable if it becomes the first or an early victim of a threat trend, which is where training and the right solutions/partner becomes invaluable.

- As a majority of organizations are heavily investing in cybersecurity as well as purchasing cybersecurity risk liability insurance, institutions that are not responding in kind with their competitors risk falling behind, even if they currently have a best-in-class system. Furthermore, the increases in cybersecurity investments being made are significant, with a reported increase of 10% or more in the next 12 months by more than half of the financial services institutions surveyed. In other words, institutions that are not heavily investing now because they believe they have a best-in-class cybersecurity enterprise will find themselves as "average" or even "laggards" in a short matter of time.

- Institutions need to leverage multiple resources for assessing and addressing their cybersecurity vulnerabilities including annual performance reviews of their cybersecurity practices and policies.

About Arizent Research

Arizent delivers actionable insights through full-service research solutions that tap into its first-party data, industry SMEs and highly engaged communities across banking, payments, mortgage, insurance, municipal finance, accounting, HR/employee benefits and wealth management. Arizent has leading brands in financial services, including American Banker, The Bond Buyer, Financial Planning and National Mortgage News, and in professional services, such as Accounting Today, Employee Benefits News and Digital Insurance. For more information, please visit www.arizent.com.

Interested in learning more about how to put Arizent's full-service research capabilities to work for your company? Please contact: Janet King, Vice President Research, janet.king@arizent.com, 207-807-4806.