ASSOCIATION FOR FINANCIAL PROFESSIONALS

2019 AFP®

CYBERRISK SURVEY

Sponsored by WELLS FARGO

ASSOCIATION FOR FINANCIAL PROFESSIONALS

2019 AFP®

CYBERRISK SURVEY

The 2019 AFP Cyberrisk Survey was conducted onsite at AFP 2019, via the mobile app. The primary objectives of this survey were:

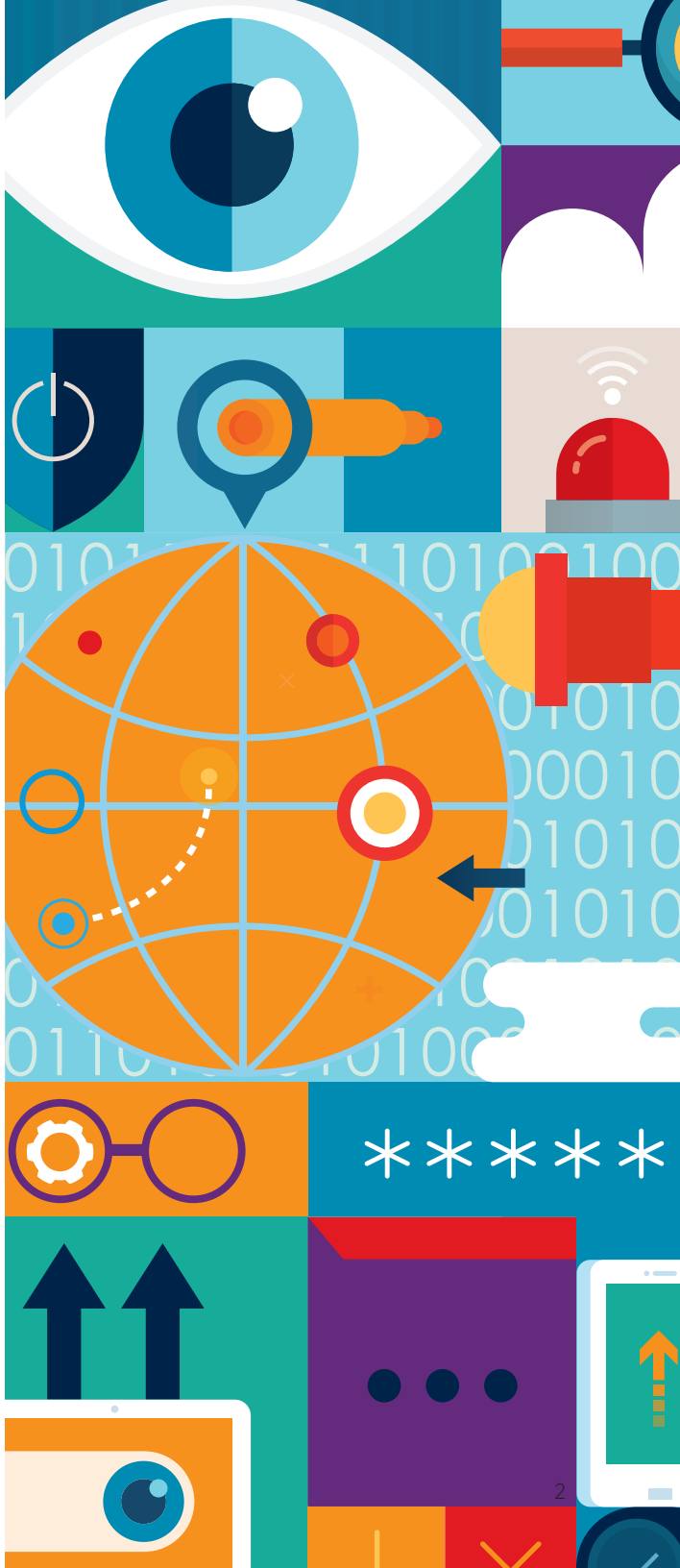
— To determine the extent of attempted or actual cyberattacks at organizations in the past 18 months.

— To identify the most severe impacts of a cyberbreach at organizations.

— To gauge the level of priority treasury and finance functions at organizations are placing on cybersecurity.

The survey received a total of 433 responses, of which 88 percent (304) of responses were from corporate practitioners, i.e. those who execute and manage treasury functions at organizations. Responses received from the 304 corporate practitioners form the basis of this report.

AFP thanks Wells Fargo for sponsoring this survey.

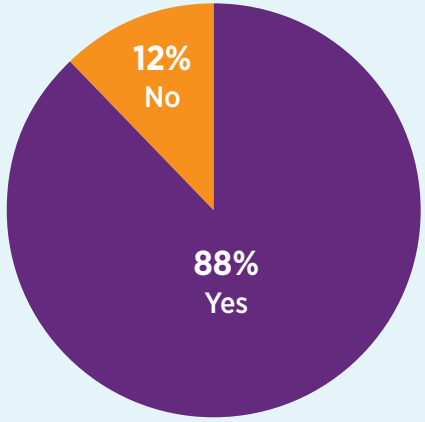


ASSOCIATION FOR FINANCIAL PROFESSIONALS

Organizations that have Experienced an Actual or Attempted Cyberattack in the Past 18 Months

(Percentage Distribution of Organizations)

A large majority of corporate practitioners reported that their organizations had been a target of either an attempted or actual cyberattack in the past 18 months. This signals that those committing these attacks are not discouraged by increasing controls and measures being put in place, or the consequences that they might face, and continue to attempt to infiltrate organization through various methods.

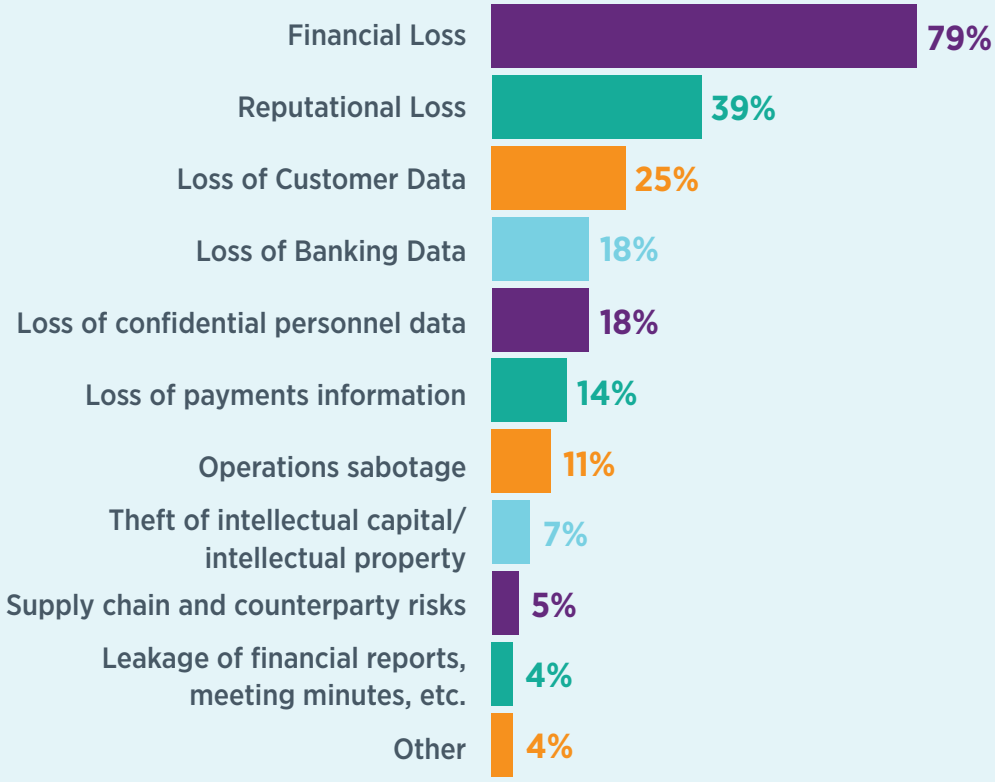


ASSOCIATION FOR FINANCIAL PROFESSIONALS

Most Severe Impacts of a Cyberbreach on Organizations

(Percent of Organizations)

Nearly 80 percent of survey respondents believe the most severe consequence of a cyberbreach at their companies has been financial losses and 39 percent are concerned about the loss of reputation arising from a cyberattack. Financial losses will impact the bottom line, and most organizations are vulnerable. Reputation loss is a greater risk to high-profile organizations. However, even lesser-known organizations are concerned about the reputational impact of a cyberbreach amongst their suppliers and customers.

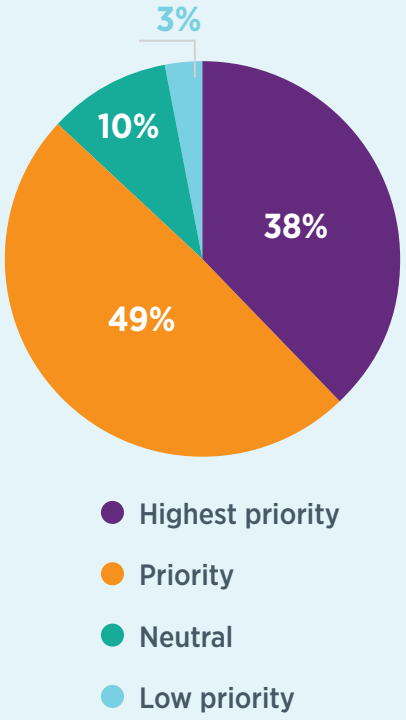


ASSOCIATION FOR FINANCIAL PROFESSIONALS

Level of Priority Treasury and Finance Functions Place on Cybersecurity, Relative to Other Challenges

(Percentage Distribution of Organizations)

Financial leaders are cognizant of the risks that cyberattacks pose to their organizations and are taking steps to mitigate these risks. Eighty-seven percent of organizations are prioritizing and focusing on cybersecurity versus other issues at their companies. Only three percent of organizations consider cybersecurity a low priority. Treasury and finance leaders are tasked with managing liquidity and risk, and attempt to do so effectively through prudent risk management practices, i.e., proper controls, while ensuring these are in conjunction with their IT department's cybersecurity protocols. Treasury teams have no option but to constantly be on high alert.

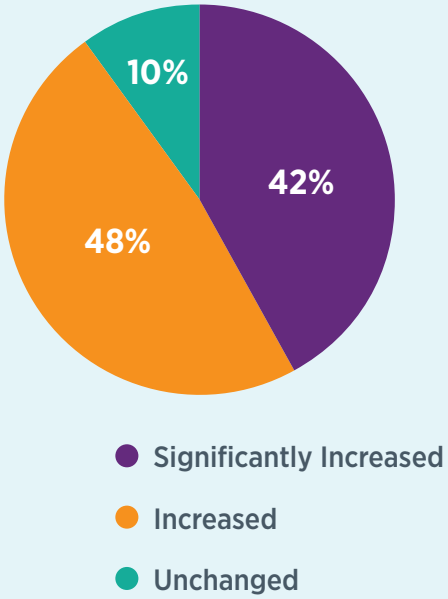


ASSOCIATION FOR FINANCIAL PROFESSIONALS

Change in Organizations' Treasury and Finance Functions Emphasis on Cybersecurity Awareness in the Last Three Years

(Percentage Distribution of Organizations)

An overwhelming majority of corporate practitioners (90 percent) report that the emphasis on cybersecurity at their organizations has increased in the last three years suggesting treasury and finance professionals are anxious about the impact of cybersecurity and making all efforts to mitigate them and keep their organizations secure. Business email compromise (BEC) scams and the rise in wire fraud are significant risks being addressed by treasury and finance leaders. They are fully aware of the need to more effectively manage their email and are training employees to follow the "trust, but verify" policy. This encourages employees to maintain open communication with senior management to validate requests, and prevents companies from being victims of BEC scams. Additionally, in an effort to minimize organizations from being victims of these attacks, corporate practitioners are increasingly terminating using email for transaction approvals.

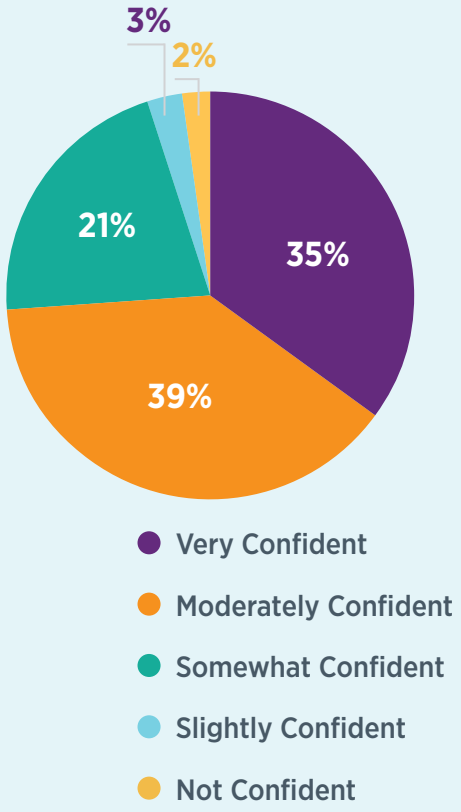


ASSOCIATION FOR FINANCIAL PROFESSIONALS

Level of Confidence that Organizations are Better Prepared to Manage and Respond to a Cyberattack Today

(Percentage Distribution of Organizations)

Though there appears to be high levels of concern among corporate practitioners regarding the prevalence of cyberattacks at their companies, only 35 percent of survey respondents are very confident that their employers are better prepared to manage and respond to a cyberattack today than they were three years ago. Thirty-nine percent are moderately confident of their organizations' preparedness to manage a cyberattack and 21 percent are somewhat confident. Senior management may need to step up their efforts to mitigate cyberattacks and demonstrate to their employees that they are thoroughly prepared to manage an onslaught of these attacks.



2019 AFP®

CYBERRISK SURVEY

Conclusion

These results suggest that hackers targeting organizations are relentless. Attempted/actual cyberattacks are pervasive and the risk of them occurring is very high. Financial leaders are focusing much of their attention on safeguarding against these attacks, which typically requires a significant use of resources. This might mean shifting resources away from other projects. Organizations need to stay ahead of those committing these crimes and have measures in place to detect cyberattacks at an early stage to prevent their companies from being vulnerable. Educating and training employees can also help keep these attacks to a minimum. However, it's often hard to remove the human element completely, which is either a result of social engineering or due to a lapse in judgment.

It could very well be that hackers will make any and all attempts to outsmart barriers that organizations have in place. With the advancement of technology, they might be more successful in committing cybercrimes than previously anticipated. Therefore, the 'new normal' for treasury and finance leaders is being cognizant of potential attacks. Treasury and finance professionals must remain vigilant, collaborate with their IT staff and banking partners, and utilize the most current and advanced connection protocols to thwart new threats.

ASSOCIATION FOR FINANCIAL PROFESSIONALS

AFP Research

AFP Research provides financial professionals with proprietary and timely research that drives business performance. AFP Research draws on the knowledge of the Association's members and its subject matter experts in areas that include bank relationship management, risk management, payments, and financial accounting and reporting. Studies report on a variety of topics, including AFP's annual compensation survey, are available online at www.AFPonline.org/research.

About AFP®

Headquartered outside of Washington, D.C. and located regionally in Singapore, the Association for Financial Professionals (AFP) is the professional society committed to advancing the success of treasury and finance members and their organizations. AFP established and administers the Certified Treasury Professional and Certified Corporate FP&A Professional credentials, which set standards of excellence in treasury and finance. Each year, AFP hosts the largest networking conference worldwide for more than 7,000 corporate financial professionals.

4520 East-West Highway, Suite 800
Bethesda, MD 20814
T: +1 301.907.2862 | F: +1 301.907.2864

www.AFPonline.org