2019 AFP® CYBERRISK SURVEY

Despite increased security efforts, cybercriminals aren't giving up

AFP RESEARCH

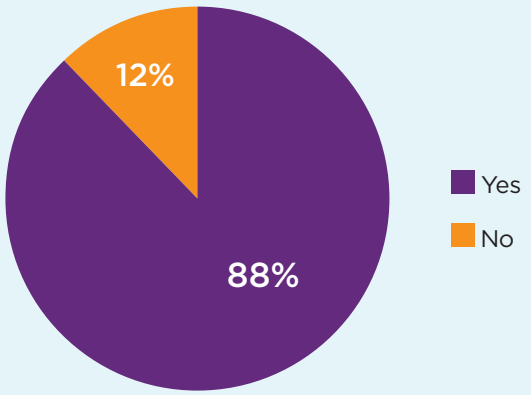
Financial professionals have significantly stepped up cybersecurity defense over the past three years as cybercriminals increase their efforts to breach organizations, according to the 2019 Association for Financial Professionals Cyberrisk Survey, underwritten by Wells Fargo.

Conducted in October at AFP 2019 in Boston, the survey garnered 433 responses, of which 88% were from corporate treasury and finance professionals. Responses received from those practitioners form the basis of the report.

Relentless attacks

Fully 88% of corporate practitioners revealed that their organizations have been targeted by attempted or actual cyberattacks in the past 18 months. This signals those committing the attacks are not discouraged by increasing safeguards and measures being put in place, or the consequences that they might face.

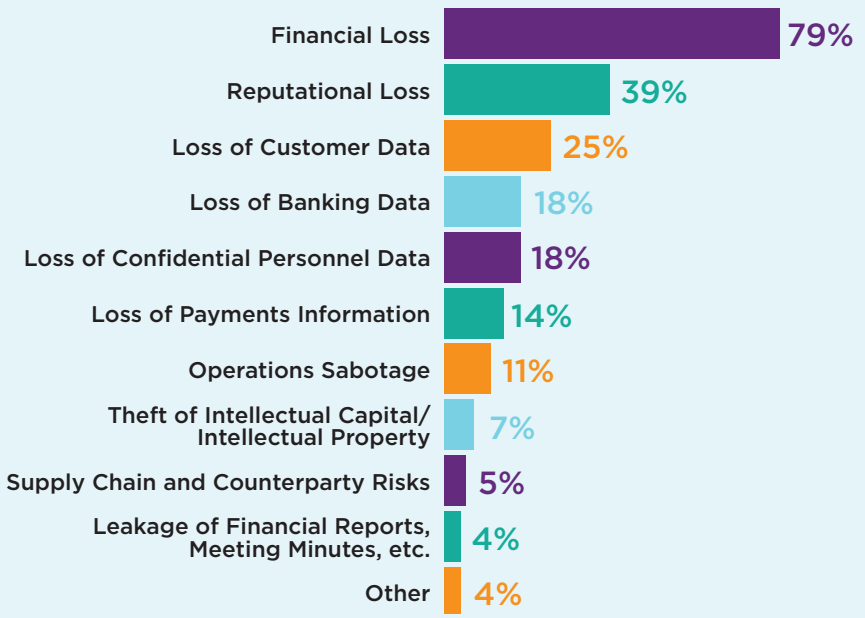
Organizations that have Experienced an Actual or Attempted Cyberattack in the Past 18 Months
(Percentage Distribution of Organizations)



Major consequences

Nearly 80% of survey respondents believe that the most severe consequence of a cyberbreach at their companies has been or will be financial losses, and 39% are concerned about the loss of reputation arising from a cyberattack. Financial losses will impact the bottom line, and most organizations are vulnerable to this risk. While reputational loss may seem to be a greater risk to high-profile organizations, even lesser-known businesses are concerned about the impact of a cyberbreach among their suppliers and customers.

Most Severe Impacts of a Cyberbreach on Organizations
(Percent of Organizations)



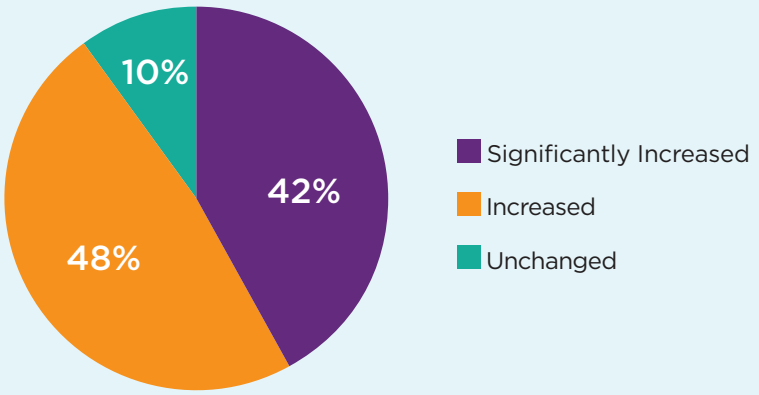
continued on page 8

Awareness

Financial leaders are cognizant of the risks that cyberattacks pose to their organizations and are taking steps to mitigate those risks. An overwhelming majority of corporate practitioners (90%) report that the emphasis on cybersecurity at their organizations has increased in the last three years.

"Treasury and financial leaders are well aware that the 'new normal' is operating in an environment where cyberattacks are frequent and cybercriminals are relentless in their efforts," said Jim Kaitz, president and CEO of the Association for Financial Professionals. "To stay one step ahead, corporate practitioners need to have measures in place that can detect attacks at an early stage, which includes educating and training employees."

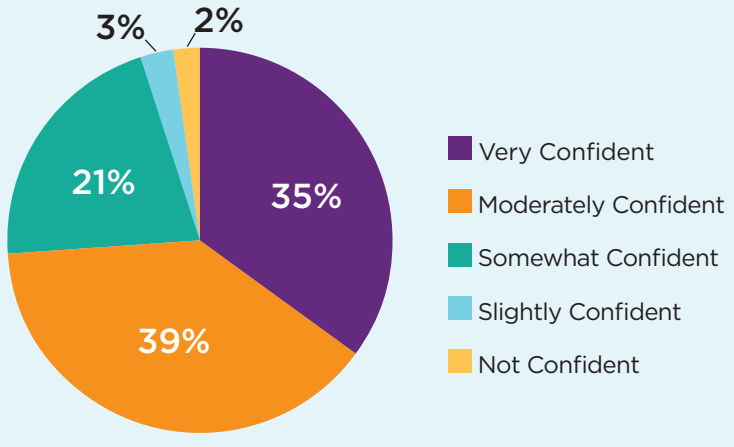
Change in Treasury and Finance Functions' Emphasis on Cybersecurity Awareness in the Last Three Years
(Percentage Distribution of Organizations)



Confidence in protections

But despite the increased emphasis on security, only 35% of survey respondents are very confident that their employers are better prepared to manage and respond to cyberattacks today than they were three years ago, while 39% are moderately confident. Senior management may need to step up their efforts to demonstrate to their employees that they are thoroughly prepared to manage these attacks.

Level of Confidence that Organizations are Better Prepared to Respond to a Cyberattack Today
(Percentage Distribution of Organizations)



Conclusion

These results suggest that 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 early 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 judgement.

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, corporate practitioners must remain vigilant, collaborate with their IT staff and banking partners, and utilize the most current and advanced connection protocols to thwart new threats.

The **2019 AFP CYBERRISK SURVEY** is available for download at:
https://www.AFPonline.org/cyberrisk