CYBER FRAUD INDEX SCORE 55

MORE INSIDE

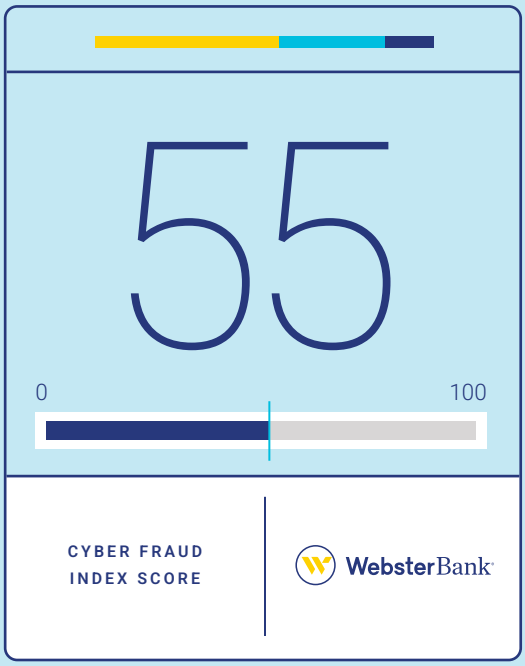
Cyber Fraud Index

AN EXCLUSIVE LOOK
INSIDE THE C-SUITE.

Webster Bank®

Our Cyber Fraud Index Score reflects executives' insecurities.

During an era of rising cybercrime, we asked C-suite executives how confident they are in their organization's ability to protect itself from cyber fraud. Our Cyber Fraud Index Score represents the percentages who answered "Very Confident" or "Confident."



WE TOOK THE ELEVATOR UP TO **THE C-SUITE** FOR A LOOK INTO HOW EXECUTIVES ARE REACTING TO **CYBER FRAUD**.

With cybercrime on the rise, Webster Bank wanted to better understand how business leaders are feeling about the risks they face, and how they're protecting their organizations.

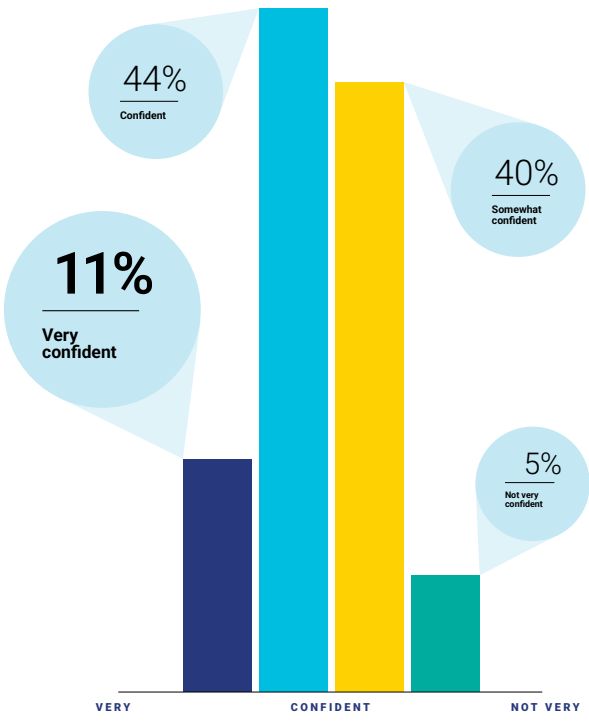
So we fielded an exclusive, intensive market study to dive into the matter, and asked questions designed to:

- **Identify** the primary concerns C-suite leaders have about cyber fraud and cybersecurity.
- **Explore** the different issues that cause them concern, as well as who they believe will be impacted by these issues.
- **Understand** the cybersecurity protection measures organizations have implemented.
- **Learn** about executives' experiences of being cyber fraud victims, as well as the impact.
- **Assess** how these leaders and organizations perceive their bank as a resource for addressing cyber fraud concerns.

Nothing's more important to Webster than the success of our business customers. And we know a big part of that depends on security. So let's take a closer look at the insights we discovered in our Cyber Fraud Index survey.

ARE C-SUITE LEADERS FACING A CONFIDENCE CRISIS?

Only 11% our respondents were "very confident" in their organization's ability to protect itself from cyber fraud.



The how and the who behind our survey.

THE CYBER FRAUD INDEX METHODOLOGY.

Our study was fielded in October 2024. It included both open-ended and closed questions, and took approximately 8 minutes to complete. **We received 150 completes from C-Suite executives**, most of whom identified themselves as one of the following:

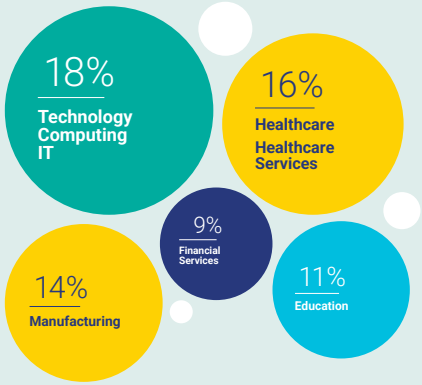
- CHIEF INFORMATION SECURITY OFFICER
- CHIEF INFORMATION OFFICER
- CHIEF FINANCIAL OFFICER
- CHIEF TECHNOLOGY OFFICER

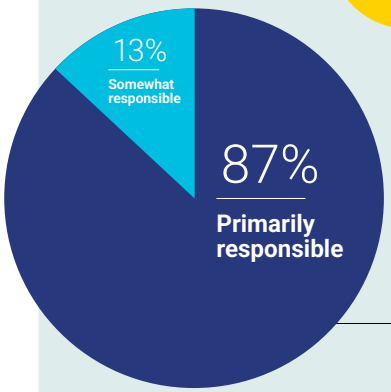
COMPANY REVENUE

Our respondents were nearly evenly split between companies above $500m in revenue and those below.

INDUSTRIES

Most of our respondents worked in the technology, healthcare, manufacturing, education and financial services industries.





LEVEL OF RESPONSIBILITY

Most of our respondents were primarily responsible for their company's cybersecurity decisions.

Insights that attracted our attention.

AN EXECUTIVE SUMMARY
OF OUR C-SUITE SURVEY.

Our Cyber Fraud Index uncovered many interesting statistics, but a few insights stood out when stepping back and looking at the bigger picture. As you analyze our results in the following pages, keep an eye out for the following themes and potential conflicts:

Tension between concerns and relied-upon resources.

Many C-Suite leaders identified third-party vendor risk as one of their top cybersecurity concerns, yet 6 in 10 still depend on third-party IT providers and consultants to protect their organizations from cyber fraud.

Cybersecurity plans vs. budgets.

91% of C-Suite executives report having a cybersecurity plan in place, but more than half also feel their cybersecurity budget is insufficient. This suggests that many executives want to do more to protect against cyber fraud but lack the funds.

High adoption of technical defenses, but low strategic guidance.

Many respondents have defenses like firewalls and multifactor authentication in place, but only about half have established a cybersecurity advisory council or a similar group to provide strategic guidance and governance on new and emerging threats.

High reliance on internal protection, but low confidence in cybersecurity.

92% of the executives we surveyed rely on internal IT resources as their primary line of defense, but less than half are fully confident in their organization's cybersecurity measures.

The desire for more bank support.

The C-Suite leaders who responded expressed a desire for banks to take a more active role in cyber fraud protection, but 40% are neutral or unsatisfied with what their banks offer them.

Resource Reliance

The majority of respondents rely on internal IT resources, but also call upon outside resources, despite concerns over third-party risks.

We asked C-Suite leaders...

What are the biggest cyber fraud risks facing your organization?

In their answers, common themes emerged: third-party risks, phishing, social engineering and ransomware. Artificial intelligence was also mentioned as a growing risk.

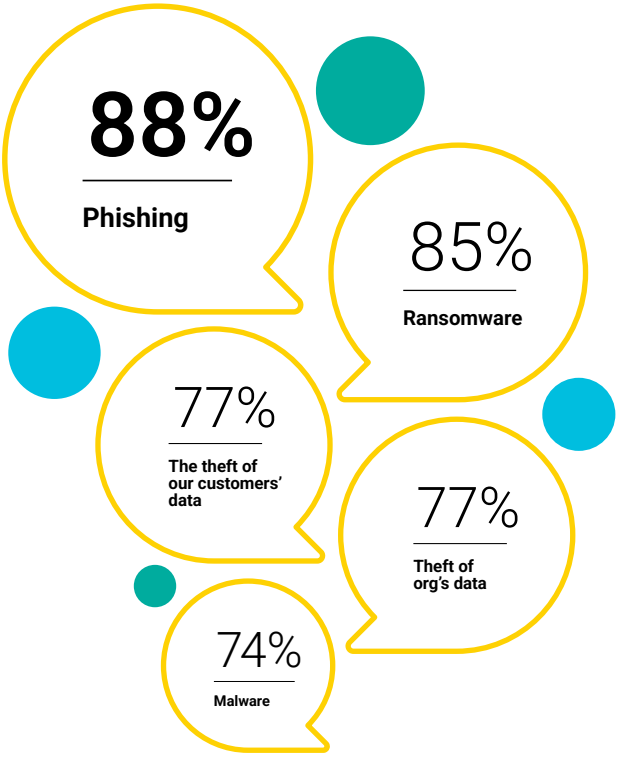
"Recently, largest risks appear to be with effective identity management, as well as **third-party risk** for subcontractors."

"The **phishing emails** to the finance people pretending to be their bosses asking to transfer money."

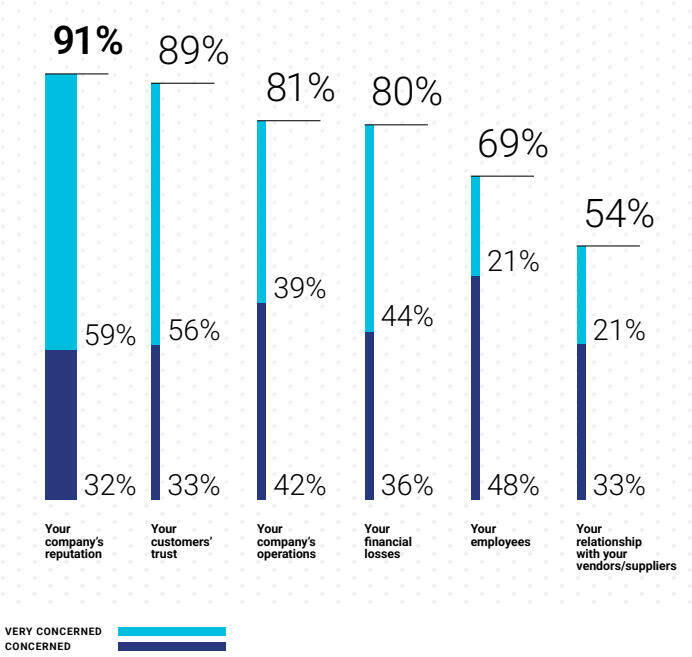
"Customer data loss, reputation loss, **ransomware attacks**, service disruption."

Top Cyber Fraud Concerns

The executives we surveyed are most concerned with phishing, ransomware and the theft of their customers' data. Theft of organization data and malware were also top concerns.



THE IMPACT



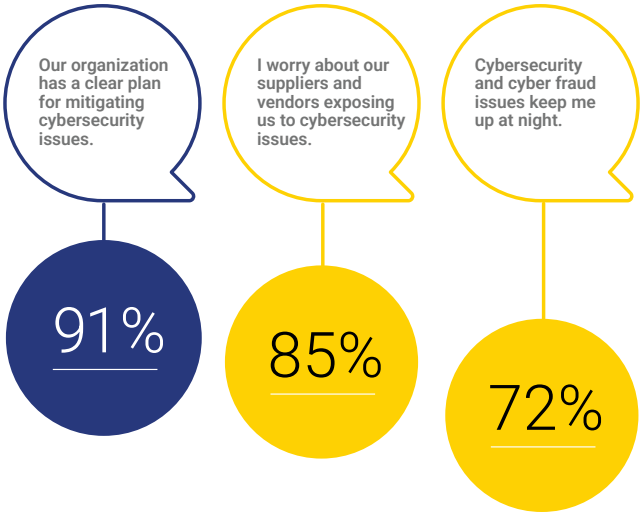
TOP CONCERNS ABOUT CYBER FRAUD'S IMPACT

We asked executives what they were most concerned with in terms of the impact of cyber fraud. **Many were worried about their company's reputation and customer trust.**

CYBERSECURITY STATEMENTS

When asked to choose from various statements related to cybersecurity and cyber fraud, many C-Suite leaders said they had cybersecurity plans, but still worried about risks.

STATEMENTS

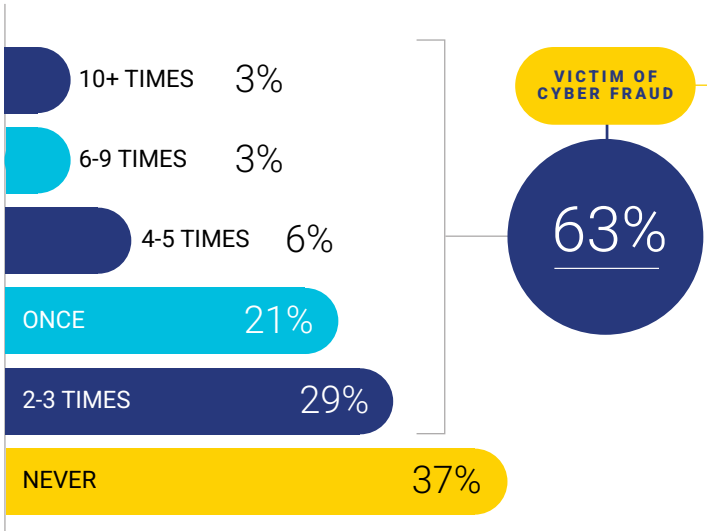


Note that while few executives feel that cybersecurity issues are out of their control, more than half don't think their cybersecurity budget is adequate.

CYBER FRAUD INCIDENCE

63% of executives we surveyed reported experiencing cyber fraud one or more times in the past two years.

NUMBER OF TIMES COMPANY HAS BEEN A VICTIM OF CYBER FRAUD



LOSSES

51% of respondents reported losses between $10,000 and $500,000 from their most significant cyber fraud incident, while 11% reported losses exceeding $1 million.

We asked C-Suite leaders...

What are the most valuable steps your organization has taken to prevent or minimize cyber fraud?

Many answered with training and education for their employees, as well as using third-party vendors — despite many being concerned by third-party risks. Multifactor authentication (MFA) and zero-trust architecture were also frequently mentioned.

"Launch of **company-wide training** on cybersecurity, which is mandatory for all employees."

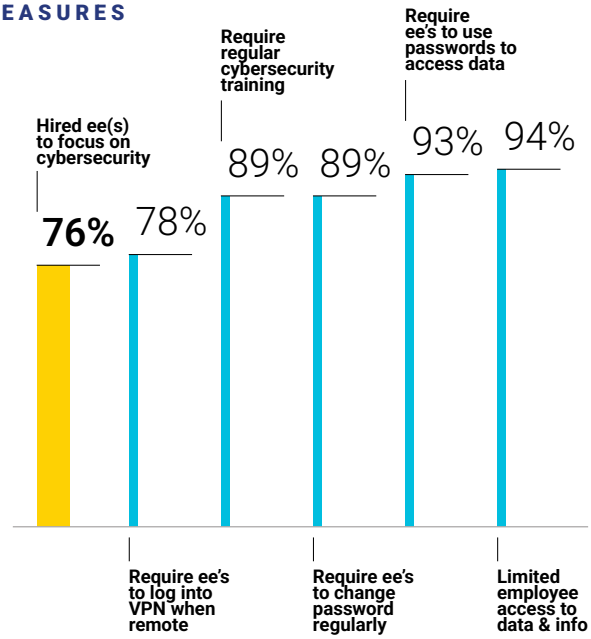
"Using **zero-trust architecture**...has forced a process of verification and authentication based on behaviors and triggers."

"**Third-party software** to prevent cyber risks."

Protection Measures Taken for Employees

Almost all executives restrict employee access to data and information, and require passwords and regular password changes. **3 out of 4 have hired employees who focus on cybersecurity.**

PROTECTION MEASURES



ORGANIZATIONAL PROTECTION MEASURES

PROTECTION MEASURES TAKEN ORGANIZATIONALLY

Two-factor authentication and firewalls are the most common cybersecurity approaches taken. **Only half of respondents have established an advisory council to address cyber fraud issues.**

We asked C-Suite leaders...

Is there any other cybersecurity support you wish your bank would offer?

The C-Suite leaders we surveyed said they'd like their business bank to be more proactive in monitoring and sharing alerts. Others want more insights into their bank's policies on cybersecurity and cyber fraud, as well as auditing and consulting services.

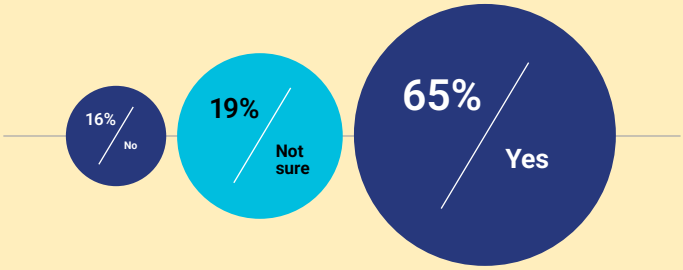
"Peace of mind and added security free of charge, **proactive monitoring**."

"I would like them to provide more **details on how they are protecting us** and their customers from cyber fraud."

"A **real-time page** where we can monitor our data, accounts and money."

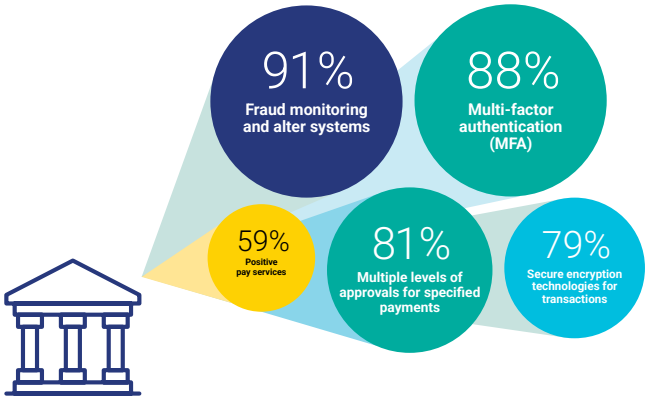
Bank Fraud Protection

Nearly two-thirds of respondents said their bank offers fraud protection services. **20% weren't sure.**



SERVICES OFFERED BY YOUR BANK

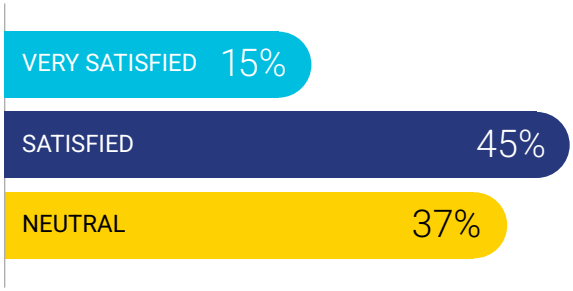
Nearly all executives confirmed that their bank offers fraud monitoring services and MFA. **Only 59% said their bank offers positive pay services.**



SATISFACTION WITH FRAUD PROTECTION SERVICES

60% of C-Suite leaders were satisfied or very satisfied with their bank's cybersecurity support, but **40% were either neutral or unsatisfied.**

SATISFACTION WITH BANK SERVICES



CONCLUSIONS

OUR RECOMMENDATIONS FOR EXECUTIVES, BASED ON THE INSIGHTS REVEALED IN OUR RESEARCH:

Elevate the role of cybersecurity within your organization and decision-making.

Shift your organization from reactive to proactive cybersecurity approaches.

Support collaboration between your internal teams, external vendors and your business bank.

Establish rigorous monitoring and vetting processes for third-party relationships.

These steps can help you both minimize immediate cyber fraud risks and build a forward-looking, resilient cybersecurity infrastructure that's more able to evolve alongside emerging threats.

WE CAN HELP YOU STAY AHEAD OF CYBER FRAUD.

Webster Bank offers proactive support tailored for our banking partners. Visit our **Cyber Security Center** today to see how we can help you and explore exclusive reports and intelligence from our cybersecurity experts.