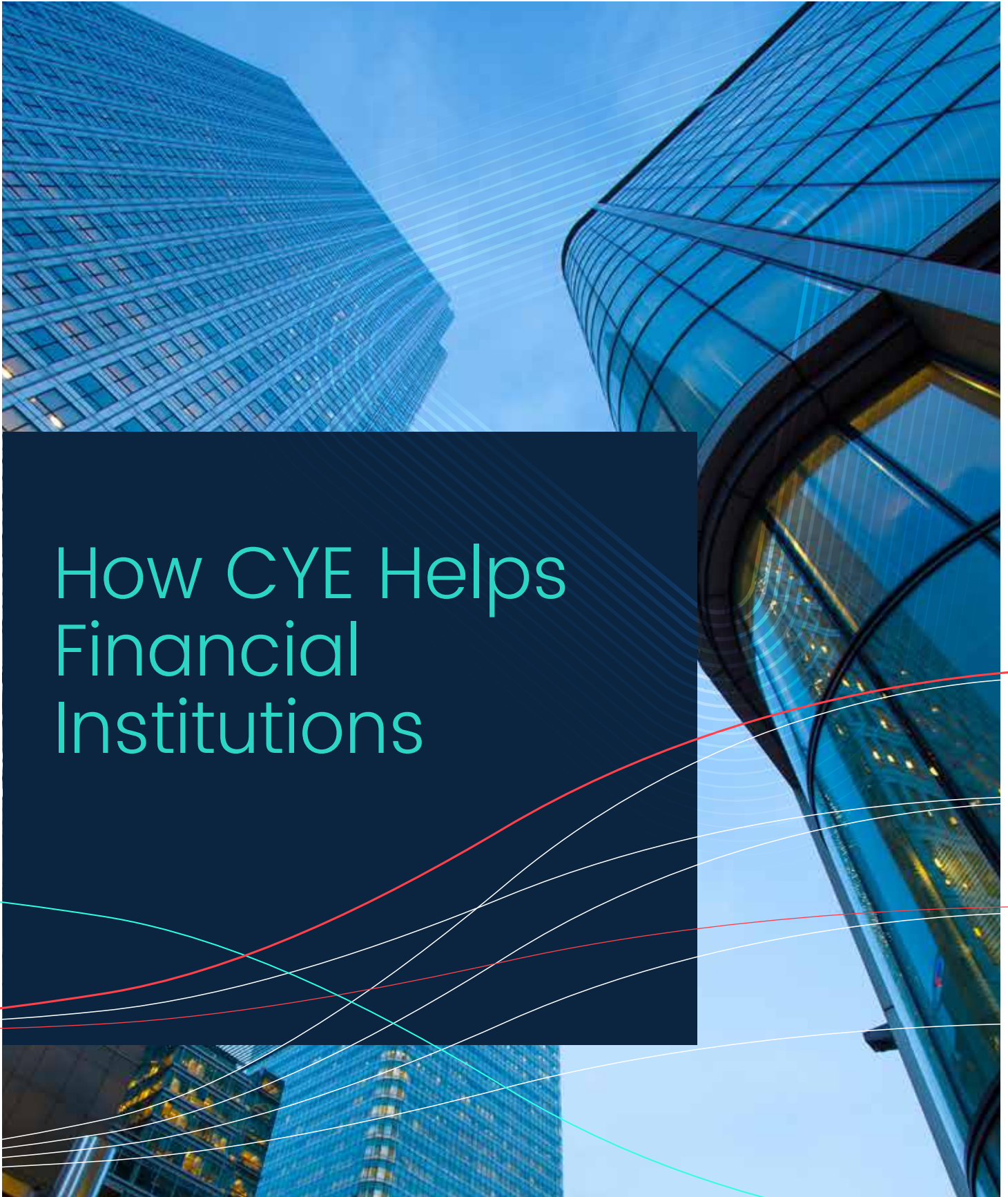




Assess, quantify, and mitigate your cyber risk

# How CYE Helps Financial Institutions



# THE SIGNIFICANT THREAT OF CYBERATTACKS TO FINANCIAL SERVICES



Financial institutions such as banks, insurance companies, and investment firms are justifiably concerned about cybersecurity. Cyber incidents threaten organizational stability and reputation and can result in significant financial burdens, including regulatory fines and penalties.

In recent years, the level of risk and likelihood for exposure has been exacerbated by digital transformation initiatives, accelerated by customer demand for cloud-driven banking and insurance services to cater to work-from-home culture. While financial institutions rely on technology and data to provide these services, they face an ever-changing regulatory environment in data protection and privacy. For example, New York's NYDFS, Europe's EBA, Canada's OSFI, and Singapore's MAS-TRM all establish and demand rigorous cybersecurity standards for financial institutions such as monitoring service providers, performing periodic risk assessments, and filing timely reports. Thus, this digital and innovation acceleration has led to several trends, including more complex cyber claims, more expensive losses resulting from cyberattacks, more financially damaging ransomware incidents, and a rise in nation state-sponsored attacks.

Managing the cyber threat landscape across technology, people, and processes has become more difficult since digitized banking and insurance services have effectively increased the attack surface, giving rise to a higher likelihood of a breach. In addition, although most financial services organizations invest heavily in cybersecurity, they continue to use the same resources, tactics, tools, and procedures to try and achieve a state of cyber resilience. They are failing, for many reasons: legacy cyber strategy, an outdated cyber technology landscape, a plethora of ineffective technologies, time-to-market demands of business, and more.

Unfortunately, many financial institutions are still getting caught in the trap of believing that buying a shiny new tool with all the bells and whistles without changing behavior is going to solve these problems. They do not realize that real cybersecurity is not about the amount of vulnerabilities and misconfigurations, the speed of mitigating the most critical CVEs, the number of Red Teams, or the extent of SOC capabilities. True cyber transformation requires a 180-degree turnaround, and CYE is at the forefront of this revolution in financial services.



There needs to be a shift in attitude from pure prevention—which is no longer realistic—to fully understanding a company's exposure to cyber risk. Putting the cost and likelihood of a potential breach into financial terms is more important than ever for organizations.

Reuven Aronashvili  
Founder & CEO



# HOW CYE TRANSFORMS CYBERSECURITY OPERATIONS IN FINANCIAL SERVICES

Since its inception, CYE has specialized in cybersecurity for financial services, providing customers with contextual business insights so they can make the best security decisions for their organizations.

CYE's SaaS solution forecasts attack routes and correlates technical vulnerabilities with business insights that optimally reduce cyber exposure through scientific analysis of the organizational risk profile. It accomplishes this by using advanced algorithms and graph modeling, aided by expert Red Teams with national-level experience. The system then assigns a dollar value to each possible breach and indicates exactly where mitigation is needed and how much it will cost.

These assessments and services are unique for each financial services organization and are based on an algorithm using the most relevant and up-to-date data. CYE thus delivers a real picture of the risk scenarios banking and insurance companies face and the bottom-line effect it could have on the business.

CYE uses these insights to develop cybersecurity strategies for financial services organizations by using a "slow down to go faster" approach: It works closely with customers to define an initial scope of valuable services that are both achievable within a reasonable period of time and repeatable across the organization. Using this approach, CYE works with customers to transition existing resources, workloads, and inefficient utilization of cybersecurity funds to a focused and optimized risk quantification strategy based on real threats and their associated risks. By enabling financial services organizations to assess, quantify, and mitigate their true cyber risk, CYE helps protect companies and enable business.

## CASE STUDY:

### HOW CYE HELPED A GLOBAL BANK CUT ITS BUDGET BY 27%

Following a series of data breaches of financial institutions, a global bank contacted CYE to validate that it was fully protected against various cyber threat actors and attack strategies. CYE's combination of Red Team experts and AI technology allowed the organization to continuously monitor its cyber exposure, diagnose vulnerabilities, and develop a cost-effective mitigation plan.

CYE's comprehensive 12-week assessment over more than 5,000 servers included manual and automatic attacks, remote and on-site engagement, and a Black Box approach.



The nature of cybercrime is constantly changing, and every area of the business has a responsibility to protect the organization and our customers. Our security teams are well trained, but it is still very challenging to know where the next attack might come from. This is where CYE comes in.

CISO, Global Bank



By working with CYE, the bank received:

- An objective and comprehensive assessment report, as well as a digestible and communicative dashboard to present to decision-makers
- A cost-effective mitigation plan prioritized according to the severity and exploitability of threats and potential business impact
- Streamlined remediation with actionable recommendations to close security gaps
- End-to-end validation of security measures and their effectiveness
- Access to CYE's Hyver platform, including its dashboard, mitigation planner, findings, and more



A few months after it began implementing the mitigation plan, the bank was able to make better-informed decisions about resource allocation. This resulted in removing unnecessary technologies and improving existing processes, allowing the bank to reduce its cybersecurity budget by 27%.

Would you like to learn more about how CYE can help protect your financial institution from cyber threats?

Contact us



## ABOUT **CYE**

CYE's cybersecurity optimization platform enables businesses to assess, quantify, and mitigate cyber risk so they can make better security decisions and invest in effective remediation. CYE combines this with dedicated professional guidance and advice provided by established cybersecurity experts. The company serves Fortune 500 and mid-market companies in multiple industries around the world. With headquarters in Israel and offices in New York and London, CYE is funded by EQT Private Equity and 83North. Visit us at [cyesec.com](https://cyesec.com).

Trusted by



## THE GUIDE TO CHOOSING A CYBER RISK QUANTIFICATION STRATEGY

[Read more](#)

