The bridge to possible

Cisco Financial Services Thought Leadership

Securing a resilient financial services enterprise

The bridge to possible

Securing a resilient financial services enterprise

The resilience of financial services infrastructure is critical to the functioning of global economies. Managing risk has never been more important as external and internal factors impacting financial services infrastructure have grown in scale and speed. Over the past 20 years, the industry has navigated through unprecedented and unpredictable events that created significant credit, market, and operational risks.

Today's financial institutions require a more resilient operating model that has the capability to reduce risk at scale and protect the business amid unpredictable change. This will require institutions to address new cyber risks associated with the digital expansion of financial services, an increasingly distributed workforce, and the use of the cloud for competitive differentiation.

Changing regulatory landscape

Cyber risk is the largest and fastest growing operational risk within financial services, which has the distinction of being one of the most targeted industries by cybercriminals. The significant implications of a data breach have ensured financial services' high level of cybersecurity proficiency, protection, and alignment with standards such as the International Standards Organization (ISO) 27000 series on IT risk and the U.S. National Institute of Standards and Technology (NIST) Cyber Security Framework.

Recently, regulatory agencies responded to increasing cyber risks with updated guidance for institutions and auditors. The FFIEC issued an update for U.S. banks to the Architecture, Infrastructure, and Operations Examinations Handbook as well as guidance for Authentication and Access to Financial Institution Services and Systems. These updates were meant to address expanding risks related to digital financial services capabilities including access, authentication, cloud computing, and services provided by third parties. In the United Kingdom, the Financial Conduct Authority (FCA) issued initial guidance for institutions considering remote or hybrid work in advance of future regulatory audits. Similar actions by regulatory agencies and central banks are taking place globally.

The FFIEC

The Federal Financial Institutions Examination Council or FFIEC is a formal U.S. government interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions. It created the widely used Cybersecurity Assessment Tool to help financial institutions assess their cybersecurity readiness.

Cisco has available the following overview of FFIEC tools.

- An introduction to Understanding FFIEC Regulations
- FFIEC Cybersecurity Maturity Assessment Tool
- The FFIEC's Architecture, Infrastructure, and Operations Book

The bridge to possible

The Financial Services Information Sharing and Analysis Center (FS-ISAC), an industry consortium of 7000 financial institutions, expects cyberthreat activity to increase as cybercriminals search for zero-day vulnerabilities.

Social engineering, malware, and Distributed Denial of Service (DDoS) attacks are the most common persistent threats across the industry. The FS-ISAC's predictions for 2022 and beyond reflect the challenging cyber risk environment for financial institutions:

- Nation-state cyber campaigns will mirror geopolitical tensions
- Nation-states will influence the financial services supply chain
- Ransomware groups will continue to professionalize
- Third-party risk will continue to threaten financial firms
- Zero-day vulnerabilities will increase
- Regulators will tighten the reins
- Incident response will mature

Digitization and rising complexity

The acceleration of digital has heightened awareness of associated rapid IT changes and rising complexities. This is the number one cybersecurity challenge for financial institutions, according to the Deloitte Center for Financial Services and the FS-ISAC. The growing use of cloud, data analytics, and AI/ML in the development of new products and services, and the necessity of supporting remote and hybrid work environments, have expanded the scope and scale of what must be protected.

IT and operational risk leaders are focusing on "security by design" approaches to manage this growing footprint and reduce the rising complexity of orchestrating security across many disparate security solutions. Security professionals need capabilities that can scale across an institution, providing a comprehensive, integrated, and manageable solution. The objective is to increase security visibility, anticipate what's next, take the right action, and strengthen institutional-wide security resilience investments.

The rapid acceleration and adoption of digital increases complexity

The bridge to possible

Securing the financial enterprise

The Cisco® Secure portfolio provides world-class security from the cloud edge, across networks, applications, and workloads, to end users and devices.

- Cisco Secure XDR offers Extended Detection and Response (XDR) capabilities that provide visibility and actionable insights to help security teams hunt, investigate, and remediate threats.
- Cisco Secure Connectivity provides Secure Access Service Edge (SASE) capabilities, combining networking and security functions in the cloud to deliver seamless, secure access to applications, anywhere users.
- Cisco Zero Trust offers a comprehensive solution to secure all access across your applications and environment, from any user, device, and location.
- Cisco Secure Firewall helps you plan, prioritize, close gaps, and recover from disaster stronger. With employees, data, branches and offices located all over, your firewall must be ready for anything.

Takes partners

While cyber risks will continue to pose challenges, financial institutions are well positioned to manage cyber risks in partnership with industry peers, regulators, and security solution providers like Cisco.

For more information

To learn more about financial services and technology, visit Cisco in Financial Services, and to learn more about security resilience, visit our security resilience page.

C11-3578322-00 04/23