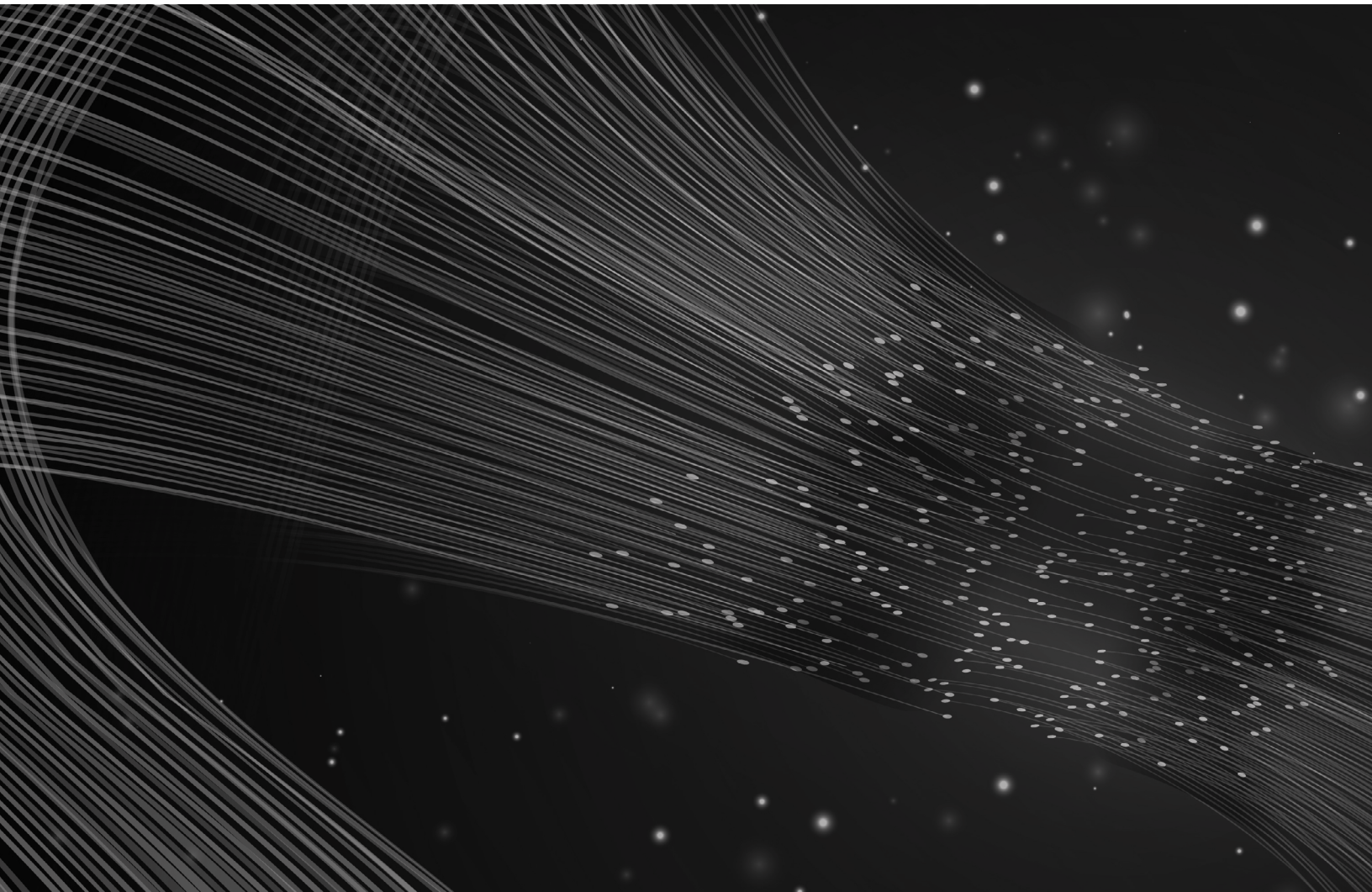
CAPCO

CYBER PROGRAM DESIGN AND COMPLIANCE REVIEW

CAPCO'S CYBERSECURITY INSIGHT SERIES



CYBER PROGRAM DESIGN AND COMPLIANCE REVIEW

Cyber programs at financial institutions need to tackle the top cyber risks to the businesses, and address expectations of various stakeholder groups. Boards, customers, regulators, and third parties alike are increasingly looking for financial institutions to address cyber risks. As financial institutions contend with ever-increasing hacks and breaches, the Board is keen to ensure that the investments in cybersecurity are being directed to tackle the top cyber risks impacting the organization. Organizations have not only had to address concerns of their Board but in light of the recent spate of significant impact and highly visible data breaches, customers are also looking to their financial institutions to define effective cyber programs. In response to the crippling effect of many cyber-attacks, regulators have also increased scrutiny on cyber programs, with bodies such as the New York State Department of Financial Services (NYDFS) mandating within the 23NYCRR500 regulation, a dedicated program to tackle cyber risk. On top of all these expectations, financial institutions also need to work as an ideal partner with third parties who could also be subject to adverse impacts resulting from any cyber risks.

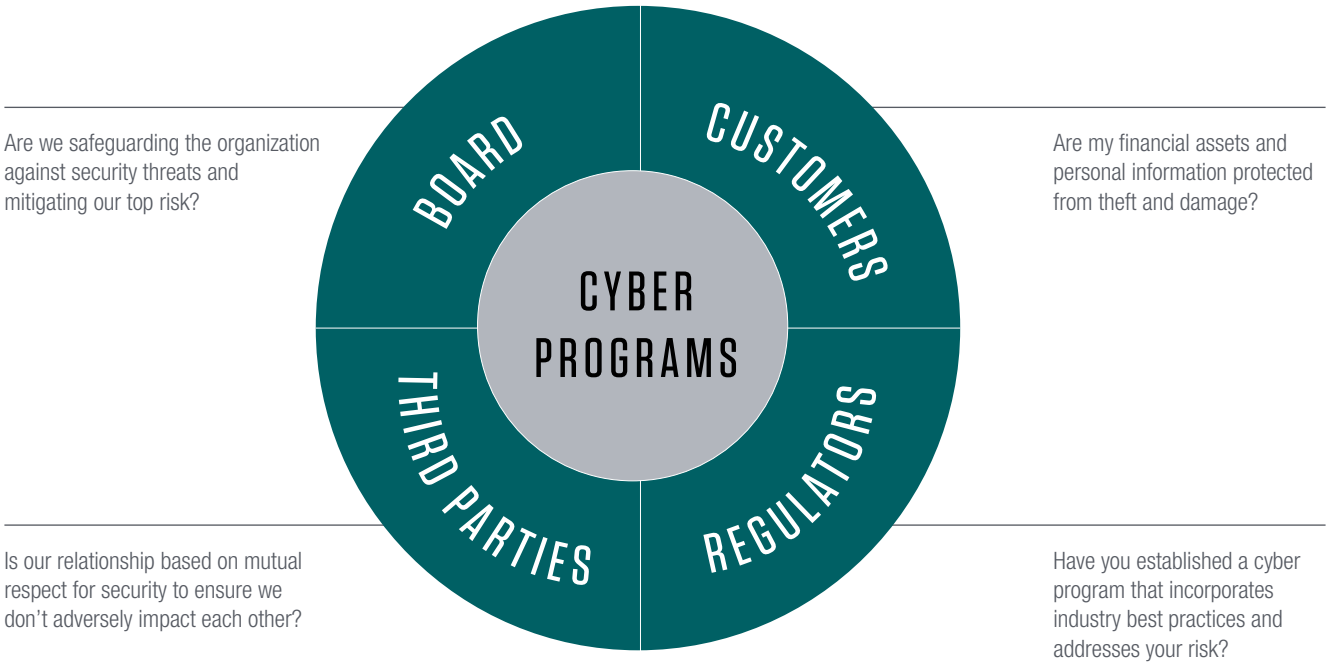


Figure 1: Expectations from cyber programs

Cyber programs need to be comprehensive and address expectations from key stakeholders, as well as be supported by an effective compliance tracking mechanism. Further, cyber programs need to be treated at par with other enterprise risk programs and enforce a culture of continuous improvement. Capco follows a five-step approach to assisting Chief Information Security Officers (CISOs) at leading financial institutions define and deploy cyber programs.

1. UNDERSTAND YOUR RISK PROFILE

One of the prerequisites for any financial institution designing an effective cyber program is to build the cyber risk profile. This requires an organization-wide understanding of the critical business products/services, supporting processes, and underlying technology assets. An evaluation of the impacts to the organization caused by disruption to these products/services, processes, or underlying technology will help the organization define its cyber risk appetite. This risk appetite is an essential input into the design of a cyber program as it will help determine the maturity requirements for the program.

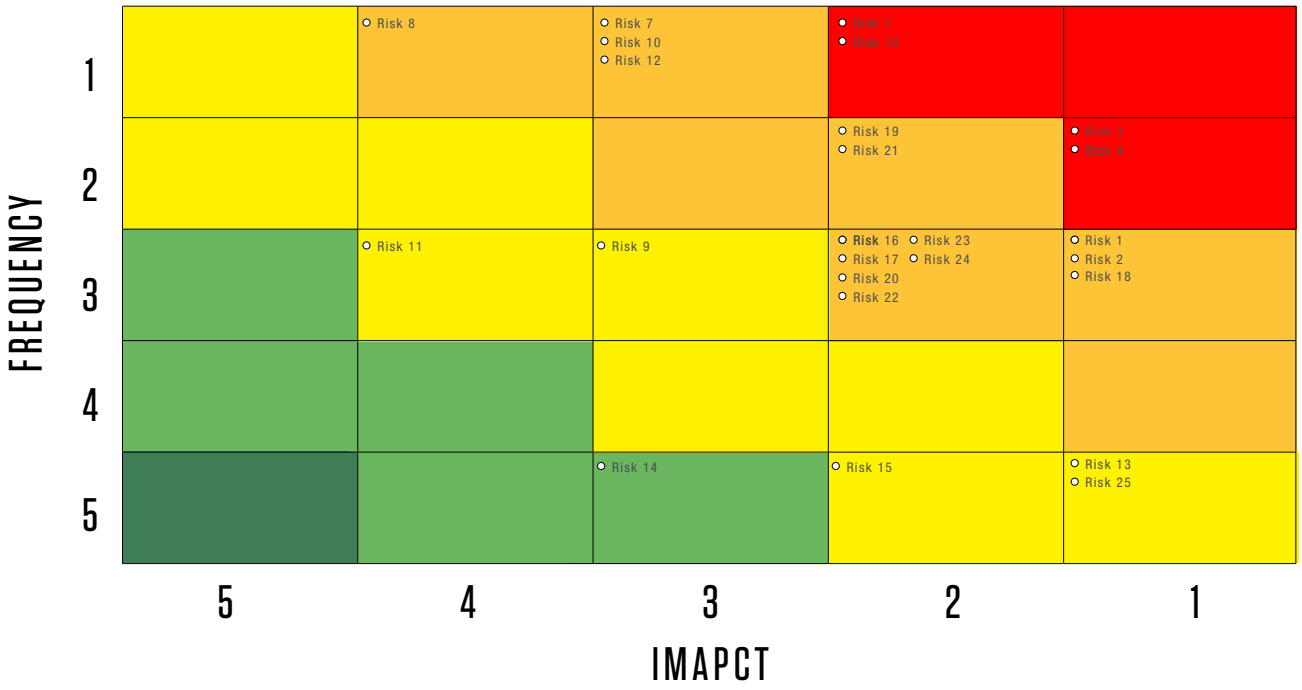


Figure 2: Cyber risks to critical business products/services

2. SET A REALISTIC TARGET

Setting an achievable target maturity helps determine the baseline requirements needed to build the cybersecurity program. To ascertain target maturity, organizations should conduct an assessment using a framework like the Cybersecurity Assessment Tool (CAT) from the Federal Financial Institutions Examination Council (FFIEC) or the Cyber Security Framework (CSF) from the National Institute of Standards and Technology (NIST). Industry groups like the FFIEC and NIST have standards to help organizations align their cyber program's maturity with their risk profile.

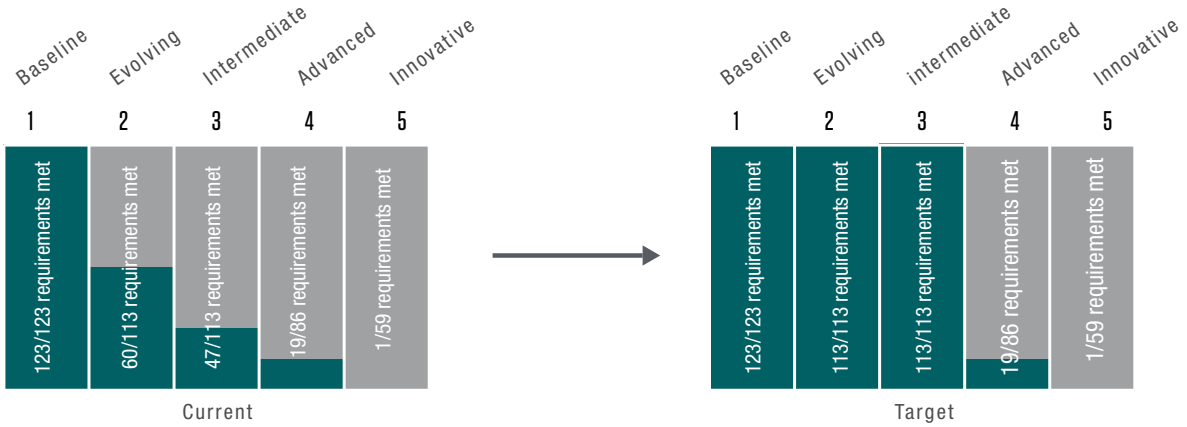


Figure 3: Setting targets for the cyber program

3. DEFINE ENTERPRISE STANDARDS FOR CYBER DISCIPLINES

Designing a cyber program to enhance the organization's security posture effectively, entails defining strategic guiding principles that can be absorbed into the organization's standard operating procedures (SOPs). The inclusion of the cyber requirements into SOPs has proven to be one of the best mechanisms to enforce security by design to be mandated across the enterprise. To build out the principles for these SOPs, organizations should take into consideration inputs from a variety of sources including policies and mandates set by management, applicable regulations, and industry best practices. These inputs can be leveraged to build an inventory of requirements that will be the foundation of the cyber program. Using the results from the maturity assessment, the organization can choose the requirements that align with its target maturity to create a set of SOPs covering relevant cyber disciplines (e.g., Identity and Access Management, Security Incident Management, Encryption, etc.). Each SOP should have an owner accountable for ensuring that the included requirements will achieve the envisioned target state of the program. Further, these SOPs should be approved by senior management and published to a central depository for accessibility by all staff.

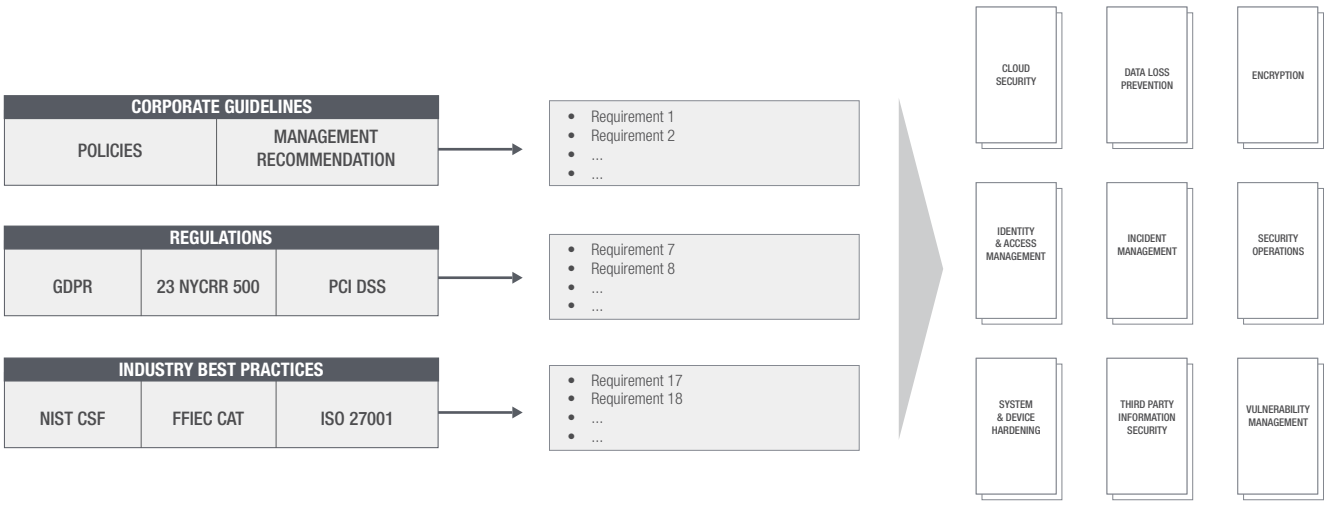


Figure 4: Standard Operating Procedures for cyber disciplines

4. IDENTIFYING MATURITY AND COMPLIANCE GAPS

Once the SOPs have been defined, approved, and published, the organization should evaluate its current level of compliance with the requirements in the SOPs, and identify where gaps exist in achieving the program target. This can be accomplished in two phases. The first is an assessment conducted in coordination with information technology and information security management to gain an understanding of which requirements are already implemented, to what extent, and which are the most significant gaps to current operations. This phase provides the organization with a high-level understanding of their current capabilities and problem areas. The second phase involves a detailed compliance review including the collection of supporting evidence. The results of these assessments will provide management and leadership teams with a heatmap of maturity challenges across the cyber disciplines and serve as an input into investment prioritization for remediation efforts.

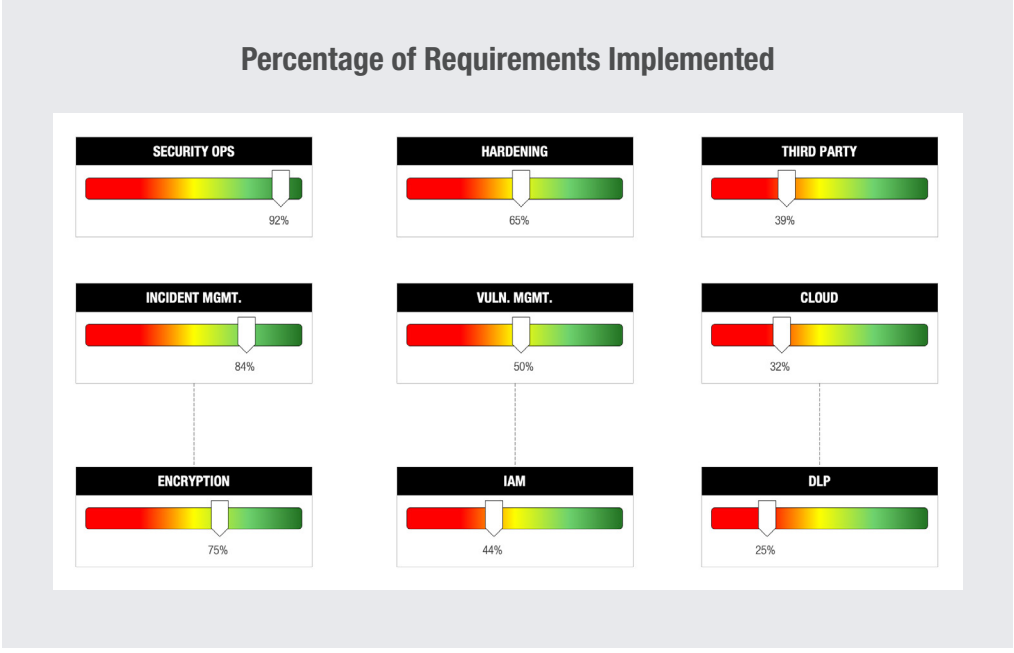


Figure 5: Maturity and compliance gaps

5. DEFINE A MULTI-YEAR CYBER PROGRAM

Often the remediation efforts to address gaps identified through the assessments will vary in size, cost, and complexity. Hence, defining a standard approach for planning remediation for the gaps is essential to the success of the program, though not always straightforward. Firstly, the gaps should be grouped together based on potential synergies to form more significant initiatives that can be examined for effort, scope, and cost. This will create a book-of-work that defines the scope of the remediation program for the next few years. The next challenge faced is determining which initiatives to address on priority and which can be deferred to the following years. Organizations should use a risk-based approach, recalling the effort performed earlier to define the organization's risk profile, and prioritize according to the impact each initiative has on risks associated with critical business products/services, supporting processes, and underlying technology assets. Initiatives that help address regulatory compliance should also be considered at a higher priority. Once a priority is established, the organization can begin to build their roadmap while taking into consideration additional factors such as budget constraints, resource capacity, and management preferences. This roadmap will become a vital tool for achieving the target maturity established for the cyber program, providing structured transition periods for organizations to implement specific controls over time.

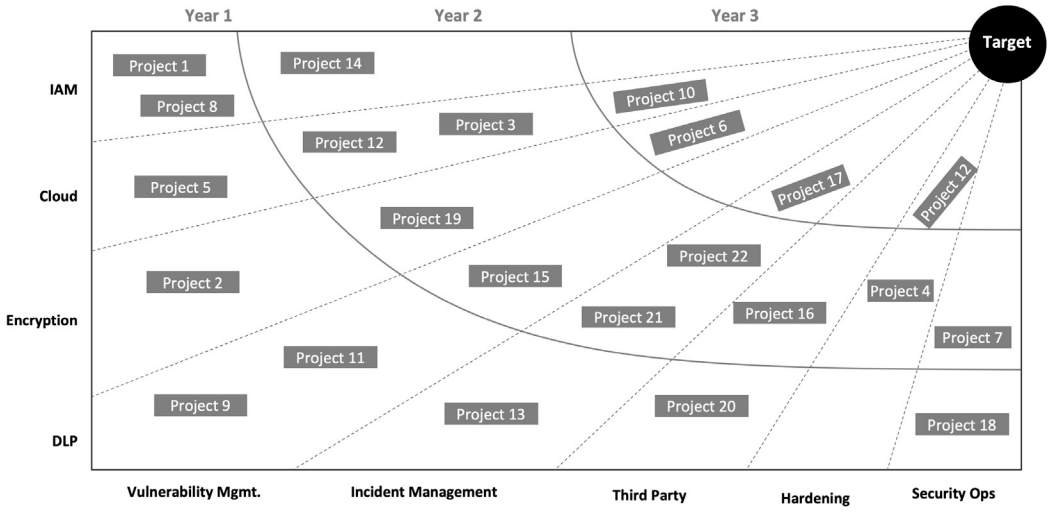


Figure 6: Multi-year cyber program

SUCCESS FACTORS

Attention to the following is an absolute must to ensure the continued success of cyber programs at financial institutions:

- Senior leadership buy-in and sponsorship of the cyber program drives a culture of the rapid adoption of industry best practices
- Non-technical aspects of cybersecurity such as business cyber risk identification, governance, incident communication, etc. deserve equal consideration to the technical components
- Single point of ownership for the SOP for each cyber discipline is critical to building accountability
- Definition of KRIs and metrics are crucial to tracking the effectiveness of the cyber program as well as providing visibility for management
- An annual refresh of the cyber program is essential to maintain the program current and address top cyber risks, management expectations, and relevant regulations

CONTACTS

Julien Bonnay
Partner
julien.bonnay@capco.com

Jayadevan Vijayakrishnan
Principal Consultant
jayadevan.vijayakrishnan@capco.com

Christopher Tecchio
Senior Consultant
christopher.tecchio@capco.com

ABOUT CAPCO

Capco's Cybersecurity Practice brings deep industry expertise, proven risk management capabilities, security technology expertise, and regulatory compliance experience. We have extensive experience advising financial institutions on strengthening their security posture by building a business case to secure funding and identifying strategic investments for the years ahead to stay ahead of the ever-evolving threat landscape.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Hong Kong
Kuala Lumpur
Pune
Singapore

EUROPE
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO
THE FUTURE. NOW.

JN_1760