Cybersecurity for Financial Services

The financial services industry is a dynamically changing environment with ever-evolving threats due to increased use of technology, growth through mergers and acquisitions as well as innovation in consumer interfaces and business processes.

Cyber breaches not only affect your bottom line, but can impact harder to measure results, and perhaps more importantly, your reputation, fiduciary responsibilities and brand.

Cherry Bekaert has decades of experience providing solutions to a diverse client base within the financial services industry, including banks ranging in size from de novo status to over $30 billion in assets.

Cherry Bekaert LLP
CPAs & Advisors

Our Risk & Accounting Advisory Services ("RAAS") Group assists financial services companies with Federal Financial Institutions Examination Council ("FFIEC") cybersecurity assessments, as well as compliance with the Gramm-Leach-Bliley Act ("GLBA") and the NIST cybersecurity framework. Our group can help evaluate your organization's information systems to assess security risks as well as IT and cyber vulnerabilities in order to help develop realistic solutions.

We offer financial services companies the following services:

- **IT and Cybersecurity Governance, Strategy, Security Planning and Policies & Procedures**
- **Security Awareness Training & Program Development**
- **Readiness Assessments**
- **Risk Assessments**
- **Vulnerability Assessments**
- **Attack & Penetration Tests/Ethical Hacking**
- **System and Organization Controls ("SOC") Services**
- **Technology and Cybersecurity Due Diligence**
- **Cyber Liability Coverage through Cherry Bekaert Benefits Consulting ("CBBC"), LLC**
- **Cybersecurity Defense & Response**

IT & Cybersecurity Governance, Strategy, Security Planning and Policies & Procedures

Minimizing the risk of cyber-attacks and securing your IT environment starts with appropriate planning at the top. Cherry Bekaert can help to define an enterprise approach for assessing, prioritizing, managing and monitoring security risks. In addition, we help define security risk tolerance posture for our clients and an approach for making cost-benefit decisions with respect to accepting residual security risk.

A large part of this is the development or update of information security policies and procedures. These documents serve as a primary element of cybersecurity and governance, and are the roadmap for your organization. They specify requirements and define the roles and responsibilities of everyone in the organization, along with expected behaviors in various situations. They must be properly created, accepted and validated by the board and executive management before being communicated throughout your organization.

Security Awareness Training & Program Development

Security Awareness Training programs are designed to provide all users of an organization with appropriate guidance on how to fulfill their security responsibilities before accessing the organization's information systems, as well as how to identify potential threats (i.e., social engineering attacks, "phishing" scams, etc.) and avoid them.

A strong IT security program cannot be put in place without significant attention given to training personnel on security policies, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to secure information system resources. Whether you need an assessment of your current program, or need help to develop one from scratch, our RAAS professionals focus on the following areas:

- Program Development & Review
- Training Materials Development & Review
- Policies & Procedures
- IT General Controls/Foundations
- Social Engineering & Cyber Awareness

Readiness Assessments & Advisory Services

Whether you are being proactive in pursuing compliance area(s) or responding to a FFIEC request, properly preparing for an upcoming review is paramount to increasing the success of an audit compliance requirement or certification.

At Cherry Bekaert, we are able to act as facilitator, interpreter, and liaison between our clients, their auditors and their regulating authorities. With our experience we are able to simplify the process of compliance and at the same time, create greater efficiencies and minimize disruptions while identifying and mitigating risks before the auditors and regulators arrive. All of this helps to eliminate distractions, confusion, and organizational stress to key personnel at your organization prior to and during the actual audit/review for the following compliance areas:

- SOC 1, SOC 2, SOC 2+ and SOC for Cybersecurity Readiness Assessments
- Technical Cybersecurity Assessments including implementation of FFIEC's Cybersecurity Assessment Tool
- FISMA/FedRAMP/NIST 800-53/171
- PCI, GLBA, ISO 27001 & 27002
- FFIEC/NCUA Readiness and Compliance
- NIST Cybersecurity
- HIPAA/HITECH/HITRUST
- Cybersecurity Defense & Response
- Privacy/GDPR

Risk Assessments

Knowing the ins and outs of your data - what types you have, where it rests, where it travels, who can access it, who can change it - is paramount to knowing your organization's security posture. Our Cyber Risk Assessments identify, assess, and prioritize threats to your organization's IT, systems, applications, and operations.

These may include security/privacy threats, fraud and abuse exposures, and inefficient/ineffective operational vulnerabilities. Our Cyber Risk Assessment group is able to provide guidance in the areas of:

- IT Security & Cybersecurity
- Data Management & Classification
- Privacy
- Vendor Management
- Mergers & Acquisitions
- Fraud & Forensics
- Business Impact Analysis ("BIA") and/or Disaster Recovery & Business Continuity Planning

Vulnerability Assessments

Every IT environment has inherent vulnerabilities. In fact, new ones are being discovered every day. The hackers know where they are; do you? Vulnerabilities can result from a variety of issues; anything from an unpatched application or operating system to a small misconfiguration in a firewall or router can put your system at risk. If these vulnerabilities are exploited, the impact can be extremely damaging. Most often when organizations fall victim to a cyber-attack, the vulnerability could have been easily avoided.

Cherry Bekaert's IT security specialists assess systems with a combination of open source, commercial, and proprietary tools to identify security vulnerabilities of external-facing systems, internal networks, or both. Our procedures are designed to confirm the existence of vulnerabilities and reduce false positives, in addition to defining mitigating solutions allowing you to shore up your environment and, ultimately, sleep better at night.

Attack & Penetration Tests/Ethical Hacking

Threats exist not only from outside the organization, but from within as well. An attack & penetration ("A&P") test, also known as "ethical hacking," is often used to determine not only the feasibility of an attack but also the impact should one of these attacks be successful. Tests are conducted by our IT security specialists to mimic how an attacker could exploit security weaknesses across multiple systems within the organization.

Undergoing A&P tests are the only way to truly understand the impact an organization could face should they fall victim to a cyber-attack. These tests go beyond identifying individual vulnerabilities. Instead, they explore the effects of a real-world attack that capitalizes on linking those vulnerabilities, which often can result in a catastrophic compromise. Without the knowledge an A&P test provides, your organization cannot fully realize the risk posed to your systems and data. Areas of focus include:

- Internal
- External
- Web Application

System and Organization Controls ("SOC"), and Attestation Services

As an independent CPA firm, we provide detailed, thorough, and well respected SOC attestations. These attest services may be used to provide assurance to applicable stakeholders that various controls can be relied upon for financial reporting ("SOC 1") or in compliance with operational criteria ("SOC 2") as specified by the AICPA Trust Service Criteria. Assurance may also be delivered in the form of other non-traditional attest services.

Our practice is experienced in:

- SOC 1 (Internal Control over Financial Reporting)
- SOC 2 & SOC 2+
- SOC for Cybersecurity
- Third Party Assurance
  - HITRUST/HIPAA/HITECH
  - FFIEC/NCUA Readiness and Compliance
  - PCI, GLBA, ISO 27001 & 2700
  - NIST Cybersecurity
  - FedRAMP/NIST 800-53/NIST 800-171
  - Third Party and Shared Assessments
- Privacy/GDPR

IT and Cybersecurity Due Diligence

In this day and age, performing due diligence related to cybersecurity for a merger or acquisition transaction should be as routine as verifying financial and legal stewardship. Cyber breaches can drastically decrease the value of a deal, even after the deal has been made. Cyber breaches, and the risks they pose, are costly to any organization. Astute investors assess the health and safety of an organization's data prior to committing a substantial investment. Likewise, a seller can benefit financially by performing due diligence to demonstrate a thorough security posture prior to sale. Third party reports on cybersecurity risk may increase investor confidence and expedite the close of a deal.

Our professionals have years of due diligence experience with:

- Cybersecurity Governance
- Administrative, Technical & Physical IT Controls
- Cyber Liability Coverage
- Cybersecurity Defense & Response
- Cybersecurity Compliance
- Cyber Risk & Vulnerability Assessments
- Technical Cybersecurity Assessments

Cyber Liability Coverage

The common opinion of today technology experts is, "It's not a matter of if you will be breached, it is a matter of when." Regulatory, legal, and notification costs related to a data breach can add up to millions of dollars. Cyber liability insurance coverage can be an effective option to transfer the risk of a breach. There are a variety of available coverage terms, policy limits, and pricing options. Cherry Bekaert Benefits Consulting's Risk Management Services practice will evaluate your exposure, current policy if applicable, and identify the most effective and efficient policy option to transfer your risk. CBBC will evaluate:

- Policy Terms and Premiums
- Levels of Coverage Relative to Quantified Risk
- Cyber Risk Transfer Clauses in Customer and Vendors Contracts

We Can Guide You Forward

Steven J. Ursillo, JR., CPA, CISA, CISSP, CEH
Partner, Risk & Accounting Advisory Services
401.250.5605
sursillo@cbh.com

Neal W. Beggan, CISA, CRISC, CRMA, CMMC-PA
Principal, Risk & Accounting Advisory Services
703.584.8393
nbeggan@cbh.com

cbh.com/cyber

About Cherry Bekaert

Ranked among the U.S. largest accounting firms, Cherry Bekaert offers assurance, tax, risk, digital, transaction advisory, benefits consulting, and wealth management solutions. With clients in across the U.S. and internationally, we have industry knowledge in technology, healthcare and life sciences, industrial manufacturing, private equity, real estate and construction, professional services, hospitality and retail, government and not-for-profit. We exercise a deliberate curiosity to know our clients' industries and work collaboratively as one team to guide them forward.

Cherry Bekaert LLP is a founding, independent member of Baker Tilly International, a top-ten global accountancy and business advisory network.

v. June 1, 2021 2:15 PM RAAS-Cybersecurity-Financial_695643988

Cherry Bekaert LLP
CPAs & Advisors