

Cybersecurity & Privacy Advisory Services

Customized Cybersecurity and Privacy Risk Mitigation Solutions

The speed with which cybersecurity and privacy risks evolve is as staggering as the magnitude of the liability associated with attacks and data breaches. From simple phishing scams to complex data security breaches, losses can be devastating in confidential, proprietary and customer information as well as in public trust and corporate image. The days when companies felt safe with passwords and firewalls alone are long gone. Today, thorough protection demands a holistic, comprehensive, integrated control system for managing risk.

To protect against these threats, PKF O'Connor Davies helps implement practical risk assessment frameworks that include continuous monitoring and real-time assessments. The specialists in our Cybersecurity and Privacy Advisory Group engineer tailored solutions to protect application information and network security, prepare for cyber breaches, disaster recovery and business continuity, and deliver end-user education.

A Sophisticated, Systematic Approach

Highly-qualified and deeply knowledgeable, our cybersecurity and privacy professionals serve as trusted advisors, providing clients with expert support protecting networks, computers, programs and data from attack, damage or unauthorized access. Employing a proprietary process for identifying vulnerabilities, they measure the security of the IT environment by simulating a malicious attack either within or outside the organization's security perimeter. This allows them to analyze the computer, network and application systems as a hacker or rogue employee would, spotting weaknesses, technical flaws and vulnerabilities. It offers a precise illustration of how a system would – or would not – withstand such an attack.

Our specialists present these findings along with recommendations for strengthening IT organizational policies, operational standards and procedures in a formal report. Then, we discuss the issues and opportunities further in an in-person meeting.

Recognizing that while our reports may be sufficient, we believe the real value is in assuring senior leadership understands the implications of the findings. Remediation is often not cost prohibitive and cost-effective solutions are identified and can be easily implemented.

Our professionals are trained to develop practical solutions that leverage existing resources (i.e., people, processes and/or technologies) to remediate any deficiencies identified. At the same time, when more problematic risk scenarios are identified, we'll recommend tailored solutions to protect multi-layered systems and those with large amounts of confidential, financial, health and other personal data.

The Advantages We Deliver

Profound Expertise

Principals and team members have strong foundations and accreditations in all aspects of information technology, privacy and cybersecurity. Constantly abreast of existing and potential threats and evolving regulations, our specialists serve as a single point of contact for all interactions, assuring heightened service and sensible cost efficiencies.

"Complete Perspective" Approach

PKF O'Connor Davies has significant experience in working with industries across all sectors. In addition to having cybersecurity, privacy and IT operational specialists assigned to the engagement, industry specific experts are also assigned to ensure that your operations are understood at a level no exclusive cybersecurity/IT audit firm could offer.

Scenario-Specific Solutions

To address all areas of cyber risk, we tailor programs to target a broad range of specific vulnerabilities. Because every organization is unique in its information security exposure and requirements, before any engagement begins we ensure that we understand the information security risks specific to the business model and the resources available to address them.

Knowledge Transfer

We have learned over the years that a key component to any engagement is the knowledge transfer that can be imparted throughout the engagement. Our goal is to educate those involved with the engagement so that they have an in-depth understanding of how risks are identified and quantified. We help to ensure that stakeholders have an understanding of our recommendations and how they will be effective in mitigating those risks.

Clear, Critical Communications

Information technology and cybersecurity have “languages” all their own. Our specialists understand both the complexities and nuances of advanced technology and are adept at translating these clearly. As a result, they are able to foster sound decision-making by senior management and board members.

Security and Privacy Awareness Support

Engineering a high level of security and privacy awareness is one of the most effective steps in protecting against cyber-attacks and handling personal information. Armed with in-depth knowledge of our clients’ organizations and operations, our specialists develop internal education programs that address specific needs, reflect employee populations, abilities and time constraints. Through these education programs, employees acquire an enhanced perception of cybersecurity and privacy and their own roles in protecting the organization and its data.

Comprehensive, Tailored Solutions

Our Cybersecurity & Privacy Advisory Services include:

- Cybersecurity Risk Assessments
- Vulnerability Assessments and Scanning
- Threat Modeling
- Network and Web Application Penetration Testing
- Virtual Chief Information Security Officer (vCISO)
- Social Engineering Campaigns
- Security and Privacy Awareness Training
 - Customized Instructor-Led or Web-Based
- Privacy Impact and Gap Assessments
- Privacy Notice Development and Review
- Privacy Regulation Compliance Support
 - General Data Protection Regulation (GDPR)
 - California Consumer Privacy Act (CCPA)
 - Family Education Rights and Privacy Act (FERPA)

Is your organization safe?

- Do you have an IT governance program?
- Is your governance program up-to-date and supportive of your business objectives?
- Are you in compliance with federal and state security and privacy laws?
- Which staff might fall prey to phishing?
- Have you tested your network’s internal and external vulnerabilities?
- Are your remote and wireless networks fully secured?
- Do you employ encryption to sensitive information assets?
- Are physical servers and equipment protected from sabotage?
- Can your system withstand a malicious hacker or trusted insider’s attack?
- Do all employee passwords meet industry and firm standards?
- Will your back-up system protect your data in a disaster?
- Have you done all you can to ensure that your cyberinsurance policy will cover financial loss?
- Do you have the ability to detect a data breach?
- Are your systems patched and anti-virus comprehensively installed, up-to-date and monitored?

- Plan Development and Reviews
 - Incident Response
 - Disaster Recovery
 - Business Continuity
- Forensic Data Acquisition and Analysis
- Server/PC/Laptop/Cloud/Mobile Devices
- NIST Information and Cyber Security
- Framework Assessments
- HIPAA Security Rule Compliance Reviews and
- Risk Assessments
- PCI-DSS Gap Analysis and Scope Reduction Assessments
- SEC OCIE Cyber Security Assessments
- FFIEC Cyber Security Assessments
- NY DFS Cyber Security Assessments and Compliance (23 NYCRR Part 500)
- ISO 27001 Framework Assessments
- Configuration Reviews
- IT Governance Development and Business Strategic Alignment
- Policy and Procedure Development

Distinguished representation in global, domestic, regional and local markets.

With over 150 partners and more than 1,400 professionals, we possess the resources to assist organizations of every type and size yet, deliver the focused personal attention that many larger firms cannot. Our renowned client service is available on a worldwide scale, thanks to our membership in the PKF International Network of accountants and business advisors, ensuring expertise wherever you take your operations and wherever you envision your growth.

Contact Us

To discover how we can help enhance your organization's infrastructure security and mitigate the risk of costly liability loss, please contact us directly:

Thomas J. DeMayo

Principal, Cybersecurity and Privacy Advisory
 CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
 646.449.6353
tdemayo@pkfod.com

Nick DeLena

CISSP, CISA, CRISC, CDPSE
 Cybersecurity and Privacy Advisory
 781.937.5191 | ndelena@pkfod.com

"PKF O'Connor Davies" is the brand name under which PKF O'Connor Davies LLP and PKF O'Connor Davies Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with applicable professional standards. PKF O'Connor Davies LLP is a licensed CPA firm that provides attest services and PKF O'Connor Davies Advisory LLC and its subsidiary entities provide tax and advisory services. PKF O'Connor Davies is a member of the PKF International Limited network of legally independent firms and does not accept any responsibility or liability for the actions or inactions on the part of any other individual member firm or firms.