Creating confident consumers

Client story

Client
Global provider of financial services technology

Sector
Technology

Project
Cyber security transformation

Client challenge

At a time when it's never been more important to protect the privacy of corporate and customer financial data, a global provider of financial services technology decided to proactively initiate a massive transformation of its cyber security capabilities to reduce the risk of exposure for the organization and its customers. The company wanted to remediate its security vulnerabilities quickly and identify and fill any gaps existing across its global corporate network. It also wanted to establish a governance model and take advantage of the latest technologies to give the company the confidence that it could operate without disruption from a future cyber security event.

Benefits to client

To better secure its online corporate data, the company is implementing a number of new protocols that:

- Provide a comprehensive assessment of mission-critical corporate applications to identify security deficiencies and gaps and provide a viable remediation road map, including detailed steps to reduce overall risk and further protect critical applications
- Develop an effective plan and road map for addressing identified deficiencies and vulnerabilities in the corporate infrastructure (e.g., servers, data technology, network) to improve the company's security posture and reduce risk
- Protect data and data flows by assisting with the implementation of leading technology like crypto key management, encryption configuration leading practices, and encryption capabilities
- Allow users to have a single sign-on with the added protection of two-factor authentication to prevent fraudulent access and significantly reduce the number of phishing attempts
- Give all customer support teams improved capabilities to further protect customer information and train teams on the intricacies of privacy guidelines around the world
- Leverage advanced methodologies and technologies like data science, process automation, and asset management to improve insight into critical security controls and capabilities and reduce risk
- Quickly identify anomalies so that managers can make more informed decisions and employees can regain trust in organization-wide reporting and metrics
- Gain an end-to-end view of the company's technology infrastructure to triage incidents and remediate vulnerabilities quickly should a future cyber event occur.

KPMG response

Working shoulder to shoulder with the organization beginning in 2016, KPMG member firm professionals have helped the company focus on strategy and governance, organizational transformation, and cyber defense.

— We established a project management office (PMO) to run the entire gamut of this multimillion-dollar cyber transformation program. We created a wide-ranging governance model and developed a full slate of metrics to measure the program's success.

— Bringing together the staffs of the CIO, CISO, and CTO functions, we established objectives, milestones, decision-making processes, and critical success factors. Soon, we were asked to lead weekly steering committee meetings composed of the top 40 most critical players to bring discipline and clarity to the transformation.

— As the company became more aware of the depth and breadth of our capabilities, our involvement grew to 10 separate work streams. We were able to increase our resources quickly, from the initial 3 senior-level professionals on site to a total of 24 seasoned consultants, accessible both on site and around the world.

— Building upon our work in the corporate security transformation, the client requested our support to further enhance capabilities in its Security Operations Center.

— In parallel to the support provided to the CIO, CISO, and CTO organizations, we supported the company's global privacy officer with an enterprise-wide upgrade to privacy policies and procedures as required under the European Union's General Data Protection Regulation (GDPR).

With these enhanced capabilities, the organization is well positioned to make bold decisions and feel confident that its cyber strategy, defenses, and recovery capabilities will protect its business and support its growth strategies for years to come.

KPMG insights

Transformation is an end-to-end process

Point solutions won't solve the problem. Transformation is a combination of people, processes, technologies, and change management programs that can stand up, build, run, and maintain security capabilities for the long term.

Internal stakeholders must play on the same team

When an organization is fortifying itself against a cyber attack, decisions must happen quickly. There's no time to waste debating alternatives. Take emotions and egos out of the situation and just let the data speak. Put the "brutal facts" on the table to better focus everyone on the common task at hand to achieve consensus quickly.

Simpler is better

More technology and more processes don't always guarantee more security. Aim for simplicity.

If you are interested in learning more about this case study, or if you are experiencing similar issues, please contact us.

Vijay Jajoo
vjajoo@kpmg.com
415-963-8698

Sarat Mynampati
smynampati@kpmg.com
973-912-6126

Erik Kuhrman
ekuhrman@kpmg.com
312-420-8818

Sreekar Krishna
sreekarkrishna@kpmg.com
480-326-6334

For more information on how KPMG can help turn cyber risk into opportunity, go to kpmg.com/us/cyber.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia