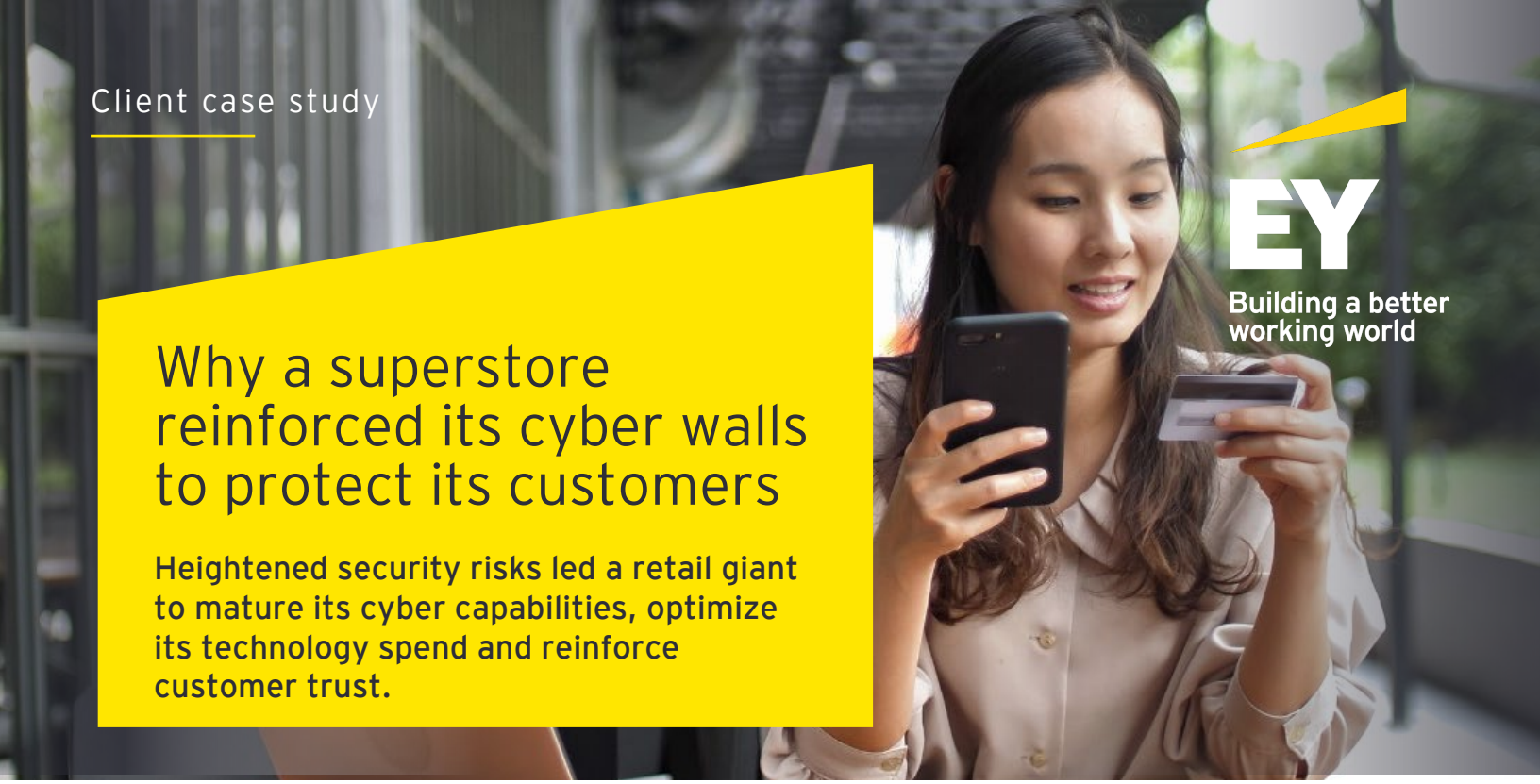

Client case study

Why a superstore reinforced its cyber walls to protect its customers

Heightened security risks led a retail giant to mature its cyber capabilities, optimize its technology spend and reinforce customer trust.

EY Building a better working world

The better the question

How can a retailer protect both data and customers?

EY's solution helped a consumer goods superstore bolster its cyber program, improve its risk posture and protect its valued customers.

1

Most major companies believe their cybersecurity systems are nailed down tight – until a surprise gust of wind blows the roof off.

Ever-changing security regulations, the global pandemic-driven spike in remote work and increasingly canny hackers all keep Chief Information Security Officers (CISOs) on high alert. In the EY Global Information Security Survey 2021, 36% of respondents reported they anticipate a major security breach that could be avoided through proactive cybersecurity investment, and 49% said compliance can be the most stressful part of their job.

"As the impacts of the pandemic unfolded, many businesses did not consider cybersecurity in their mitigation strategies, whether through oversight or an urgency to move as quickly as possible," said Abhishek Madhok, Principal, Cybersecurity, Ernst & Young LLP. "As a result, new vulnerabilities entered an already fast-moving environment and continued to threaten businesses."

An international consumer goods retailer hired a new CISO and issued a company-wide mandate to mature its cybersecurity program to combat these threatening forces. Faced with a collection of costly technology solutions and lacking a cohesive strategy to operationalize and orchestrate their capabilities, the CISO engaged EY's Cybersecurity practice to define a three-year roadmap for improving the organization's cyber posture, reducing business risk and strengthening customer trust.

The better the answer

EY helps put the customer first

Maturing cybersecurity offerings through a service-driven operating model achieves a greater return on investment.

2

Following a current-state risk assessment, a new operating model was designed to meet the goal of effectively serving customers both internal and external to the organization. The operating model centered around scalability, technology rationalization, elimination of redundant solutions and improved collaboration across the broader enterprise. The team sharpened the focus on security service delivery by developing refreshed service catalogs for internal customers, redefining roles and responsibilities, and helping to establish an interaction model to facilitate teaming.

While the operating model provided the roadmap for enacting change, a series of strategic projects were initiated to increase the organization's capabilities, impede data threats, increase existing digital security investments and mitigate security risks impacting the customer.

- Security Operations Center (SOC): To detect and combat ever evolving threats against its systems and customers, the SOC acts as the nerve center of the cybersecurity function. EY standardized and operationalized 24x7 SOC coverage for the organization, including night and weekend coverage through staff augmentation. To empower the retailer, training and mentorship were provided to staff to transition responsibility without disruption to operations. A threat-driven prioritization methodology with scenarios specific to the organization prioritized the most impactful threats, and proactive threat-hunting allowed countermeasures to be developed. These improvements to coverage and skills helped protect customers through around-the-clock vigilance. Workflows, an enhanced log and case management system matured the SOC further. Automation and migration to a cloud-native platform further optimized the SOC, which helped to properly store information and inform future decision making. A return-on-investment calculator also prioritized future SOC automation activities to achieve maximum threat reduction and manpower optimization.
- Vulnerability management: EY teams enhanced processes for the vulnerability management program by working in lockstep with IT and the business, implementing solutions to automate prioritization, orchestration and reporting of vulnerabilities throughout the organization. The new program uses a governance framework and scanning solution to revamp asset groups, tags and scan jobs. The enhancements to the vulnerability management program and scanning solution allowed for growth in the program's maturity, resulting in a more robust solution which led to a reduction of 72% of vulnerabilities across the organization.
- Identity Access Management (IAM): The organization's legacy IAM program was a patchwork of obsolete systems and manual processes supported by applications that were largely unaccounted for, leading to control deficiencies, governance gaps and risks pertaining to resource access. EY teams worked to help this retailer properly manage digital identities and establish an identity governance platform. An authoritative identity data warehouse (IDW) was built to facilitate end-to-end identity management, strengthen control effectiveness, standardize IAM processes and eliminate redundant tools. By migrating to cloud-based platforms, the organization standardized critical controls, certifications and password management and consolidated its tooling architecture to decommission seven legacy systems. This helped eliminate technology platform redundancies, as well as limited the number of access entry points. New IAM services now better protect the organization's digital perimeter by streamlining the onboarding and offboarding experience, supporting employees with secure self-service password management options and automating access provisioning.
- Technology Governance Risk and Compliance (GRC): Governance, risk and compliance should aim to be the most integrated function within a cybersecurity program, providing the foundation for good risk identification, prioritization and treatment. When EY teams were first engaged, the organization's GRC was fragmented amongst multiple cyber teams and took a controls-led approach with compliance being the top focus. Through significant collaboration and education, a risk-based, technology-enabled strategy was built for the retailer. Beginning with the current GRC technology platform, the team identified architecture modifications to better integrate the cyber risk program and help ensure identification, tracking, workflow and response were all streamlined processes. The team identified an industry standard framework to drive consistency for controls, policies, standards and to align top risks. The team educated the business on cyber risk, focusing on possible threats to operations (e.g., back office, supply chain, stores) that the retailer is facing. Future GRC maturity will continue to refine the way risk is identified and improvements to the cybersecurity posture are prioritized based on the impact to the business.

EY

The better the world works

Cloud-based data further enhances consumer trust

A cybersecurity transformation means a more secure foundation for millions of customers.

3

The multifaceted cyber-solution for this retail powerhouse created a sea change for organizational processes, policies, procedures, and technology -- which required an organization-wide adoption of new ways of working. The EY People Advisory Services (PAS) group enabled the retailer's readiness and adoption by aligning leadership, addressing the needs of their people, and minimizing disruption to critical business-as-usual activities for the organization and its customers. New communication channels and meeting forums were implemented throughout the organization to strengthen the collaboration between key technology partners, helping the organization transition the workforce to a more secure operating model. Significant communication and teaming efforts were enforced to close gaps between cybersecurity and other technology partners that historically had hindered the organization's ability to identify and protect critical assets, such as employee and consumer data, and proprietary business information.

"This international retailer needed technology enabled processes to provide its employees standardized mechanisms to manage and respond to security threats in a rapidly evolving environment," said Madhok. "The EY cybersecurity solution ultimately helped the organization protect over 100,000+ employees working across 1,000+ locations and better secured data for 1b+ customers worldwide."

Nearly three years after this cybersecurity transformation began, this superstore now has a secured foundation to combat future threats and has proactively allocated annual funding towards cybersecurity to show their continued commitment to protecting customer data, addressing future risk and building consumer confidence.

Results include:

- 1b+ customer data points better secured
- 100,000+ employees have access to newly secured data tools
- 1,000+ store locations protected with new security solutions
- 72% reduction in vulnerabilities
- 7 legacy systems decommissioned

View more EY case studies

Contacts

Dave Burg
EY Americas Cybersecurity Leader

Elizabeth Mann
EY Americas Life Sciences and Health Cybersecurity Leader

Sean Wessman
EY Americas Risk & Cybersecurity Leader

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

2303-4204113
ED None

ey.com