Moving ahead towards your digital future

Cybersecurity and privacy services

pwc

Cybersecurity and Privacy
A Board level issue

The emergence of digital technologies for delivering services is forcing companies to invest in their front office digital capabilities or run the risk of falling behind. Multiple forces such as tighter regulation, fast-paced customer demands, market shifts, unconventional foes and disruptive technologies are creating a new playing field for cybersecurity and privacy professionals. Cybersecurity and privacy is a shared problem. The Board along with the cybersecurity and privacy professionals must work together to proactively identify and manage digital disruption, regulatory upheaval and enterprise threats that the organization faces every day.

Growing Concern Over Cybersecurity and Privacy

- Increased risk of organized crime, “hacktivism”, and cyber-terrorism
- Increased media attention, and therefore brand risk, related to cyber attacks
- Increased attention for security and privacy at Board and Audit Committee levels
- Growing concern by consumers and regulators related to privacy

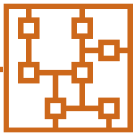
Regulatory Upheaval

- Increased number and complexity of privacy and regulatory mandates in the Philippines, the European Community, US and globally
- Increased need for integrated privacy and security to facilitate compliance with multiple regulatory requirements
- Regulators increasingly take a “due care” approach to cybersecurity & privacy.
- Regulators are imposing substantial fines and penalties for non-compliance

Adversaries

Organizational Change

- Mergers and acquisitions are on the rise
- Hyper-connected, borderless technology and business environments are increasing
- There is a rise in off-shoring models and increased reliance on third-parties to drive cost efficiencies
- Many organizations experience difficulty finding and retaining highly skilled security and privacy resources



Digital Disruption

- Mobile devices contain troves of sensitive business information and are often not well-controlled
- Digital transformation moves data outside of the walls of the business and outside of the traditional control on management
- The boom of Big Data is colliding with increased concerns and awareness over privacy
- Speed to market in the Internet of Things realm can have unintended and expensive security and privacy consequences

What's at risk?

You've heard it all before

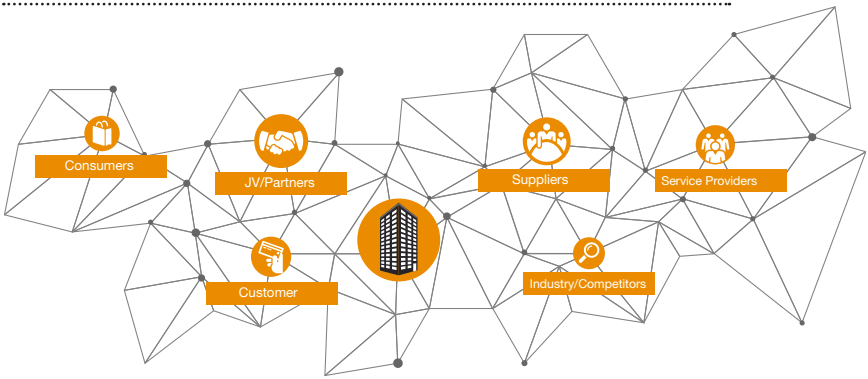
Cybersecurity incidents continue to rise. Cyber compromise is a matter of when, not if. The financial costs of a breach increases every year.

Today's elevated threat environment has left most organizations wondering if they have already been (or soon will be) compromised.

Many are deliberating how to strengthen their cybersecurity program, while others are scrambling to understand the motives of potential adversaries.

For most businesses, the resolutions to these challenges are ambiguous, at best.

The ever expanding elements of today's interconnected business ecosystem



Is my cybersecurity program up to the challenge?

This uncertain state of security has evolved in tandem with technological advances that have redefined the business landscape. Wireless networks, mobile devices and apps, social media, cloud services and data analytics have created entirely new ways for businesses to improve operational efficiencies, market products and services, and interact with customers. Together, these technologies have created a dynamic, hyper-connected business ecosystem that enables companies to share significantly more digital information with a wider range of partners, suppliers, service providers, and customers.

As innovation continues to advance and technology domains converge, the cyberattack surface–the points on which adversaries attempt to access systems, applications, critical assets, and highly sensitive information–are expanding exponentially. At the same time, traditional threats are dynamically changing like economic conditions, regulatory requirements, geopolitical instability and social demands.

What we offer

Our Cybersecurity team consists of highly trained and specialized consultants, professionals, CISOs, and industry veterans with experience helping global businesses across industries assess, design, deploy, and operate cybersecurity and privacy programs.

Vulnerability Assessment and Penetration Testing

Our Vulnerability Assessment and Penetration testing includes the conduct of internal, external and web application penetration testing assessment of your network and applications. The objectives of the testing are to comprehend the susceptibility of infrastructure components to unauthorized access from malicious insiders and outsiders and to help establish the effectiveness of your threat and vulnerability management program. The services will conclude with the development of recommendations to mitigate identified risks to an acceptable level and improve the organization's information security posture.

Social engineering simulations

It is commonly acknowledged that employees of the company are often the weakest link when it comes to IT security in an organization. The willingness of most people to help others and be service minded can make your employees vulnerable to social engineering-attacks, among others. Social engineering is the process of using psychology to encourage people to give you the information or access that you want. It involves deceit and manipulation, and can be done face-to-face, remotely but still interactively (e.g. by phone) or indirectly through technology.

Information Security Management System review

PwC's approach for an Information Security Management System (ISMS) readiness and compliance review using ISO 27001 and ISO 27002. We deliver a customized approach to fit your needs and deliver the desired results.

Cybersecurity Readiness Assessment

Cybersecurity readiness assessment focuses on assessing and validating your current state cybersecurity in comparison to peer organizations and leading industry frameworks (e.g., NIST 800-53, ISF or ISO).

Business Continuity Plan and Disaster Recovery Plan Review

Business continuity plan and disaster recovery plan review with the use of ISO 22301 provides a holistic assessment that helps develop an organization-wide resilience allowing you to survive the loss of a part or all of your operational capability due to disruptions.

Improve your posture with PwC's knowledge and know-how

Cybersecurity and privacy programs that implement the correct balance of strategy, technologies, processes, and resources can enable the business to achieve its goals while protecting the assets most critical to its competitive advantage, brand and shareholder value.

Progressive approach to maturing your cybersecurity & privacy program

Assess Your Capabilities and Develop a Strategy

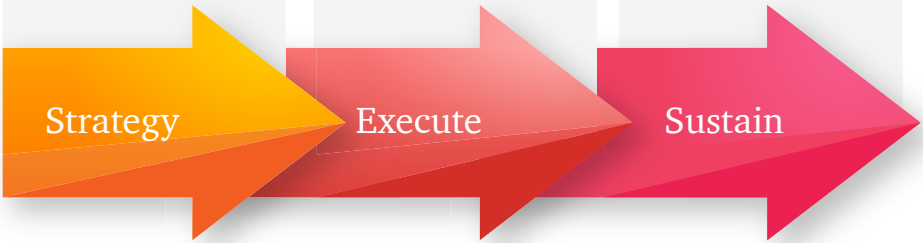
- Assess cybersecurity & privacy program maturity
- Data inventory and mapping
- Cyber risk assessment & threat modeling
- Penetration testing & breach indicator assessment
- Develop strategy and roadmap
- Organizational design

Improve Fundamentals & Transform Your Program

- Cyber risk governance
- Security & privacy by design
- Security architecture & operations
- Threat & vulnerability management
- Identity/access management
- Incident & crisis readiness and management
- Insider threat program

Manage Exposures & Sustain Program

- Cyber risk governance
- Security & privacy by design
- Security architecture & operations
- Threat & vulnerability management
- Identity/access management
- Incident & crisis readiness and management
- Insider threat program



Value delivered and benefits realized

Strategic approach

Defensible Security and Privacy Posture

Proactive & Improved Risk Management

Great confidence

How PwC can help

For a deeper discussion about cybersecurity, contact our team:

Rosell S. Gomez, CPA, CISA, CRISC, CCOBIT 5(F), CCOBIT 5(I), CRM
Risk Assurance Partner - IT
Cybersecurity and Privacy Leader
rosell.s.gomez@pwc.com
T: +63 (2) 8459 4984

Salvador C. Guarino, Jr., CPA, CIA, CISA, CISM, CISSP, C|EH, CCISO
Subject Matter Expert
T: +63 (2) 8845 2728 ext. 3487
salvador.c.guarino.jr@pwc.com

Mark Anthony P. Almodovar, CPA, CISA, CIA, CISM, CRISC, ISO27002(F), ITILv3(F), Network+, CPISI, CCNA-R&S, COBIT 5(F)
Risk Assurance Director
+63 (2) 8845 2728 loc. 3095
mark.anthony.almodovar@pwc.com

Eugene Jerome V. Tan, CPA, OSCP, eCPPT, eWPT, E|CSA, CPT+, eJPT, C|EH, C)PTE
Risk Assurance Manager
+63 (2) 8845 2728 loc. 3077
eugene.jerome.tan@pwc.com

www.pwc.com/ph

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with over 276,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.