

Cyber security

Building confidence in your digital future

April 2019



pwc

Confidence in your digital future

We believe that confidence in your digital future is essential to the growth of your organisation. It means being aware of your cyber security risks, being able to assess which threats could affect your business goals and having the agility to deal with new threats as they arise.

We look at how the world has changed and what this means as you operate in an increasingly connected world. We explore the importance of trust in your digital future and how cyber security can help you build digital trust.

We then look at the importance of focusing your cyber security investment to protect what matters most to your organisation and how historic ways of approaching security are no longer adequate. We also outline the wide range of threats that enterprises now face.

Finally we look at what you need to consider to assess the strength of your current cyber security and the steps you can take. We look at six lenses of confidence that help you to apply cyber security to the very heart of your business, where we believe it should be.

Your digital world just got bigger



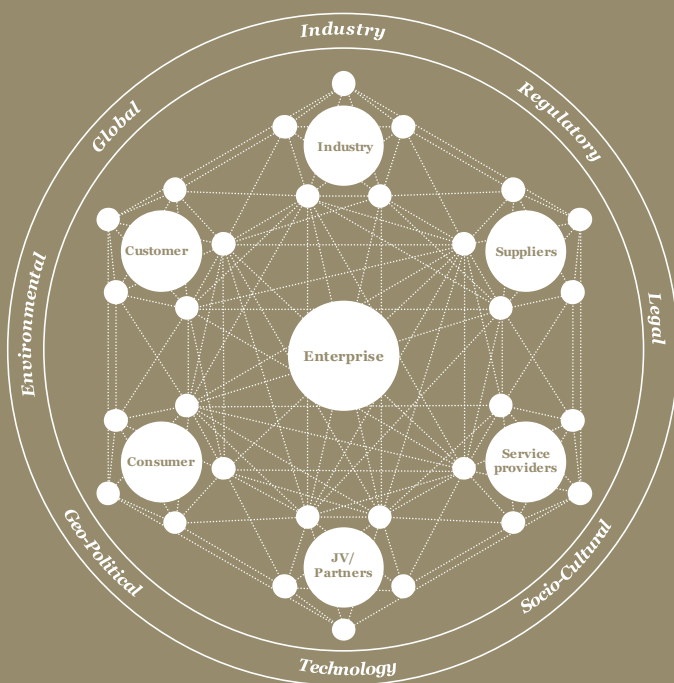
The issue

The 'digital age' is bringing rapid change: new customer connections; tighter supply chain integration; new sourcing models; new ways of exploiting bulk data; faster R&D processes; mobility; and much more. Businesses now operate in an interconnected ecosystem. As a result, securing critical data, transactions and operations means working beyond the walls of the enterprise.

The new reality:

- Increase in reliance on technology
- Organisations are built on trust and collaboration
- Information and data ubiquity throughout the business ecosystem
- Transactions and operations span multiple parties
- New and advanced threats which take advantage of the new reality

The new business ecosystem



The impact of an interconnected world

Digital technology has transformed the scope, scale and potential for business over the past decade. In doing so, it has disrupted the business models of traditional organisations at a rate never experienced before. And it won't stop there.

In an interconnected world, organisations are dependent on digital business processes. This amplifies the business impact of cyber attacks, affecting intellectual property, financial security, competitive advantage, operational stability, regulatory compliance, and reputation.

Businesses that seize the digital advantage must be confident that they are able to manage cyber security risk. Those that are able to build trust with customers and other stakeholders for their digital strategies will be successful. That is, trust that data and transactions will be safe, that identity and privacy issues have been dealt with and trust that systems and processes will be available when needed. Trust takes a long time to build but can be lost in an instant.

In short, successful businesses in the digital age will get to grips with cyber security.

Old security models are no longer adequate

While cyber security risks have evolved, the approach businesses use to manage them has not kept pace. The traditional information security model – one that is technology focused, compliance based, perimeter-oriented, and aimed at securing the back-office – does not address the realities of today.

When looking beyond the enterprise boundaries, organisations need to re-evaluate security priorities. Cyber risk management today is a complex issue, requiring board and management engagement, sophisticated techniques, and new skills and capabilities.





Businesses are facing rapidly increasing exposure to cyber security risk. Cyber security should be treated as an enterprise risk for which boards need to develop a clear risk appetite – to suit their specific business circumstances – and associated action plan; and need to seek regular assurance that risks are appropriately monitored and managed.

Cyber threats are business risks

When CEOs and boards evaluated their market threats or competitors, few previously considered cyber threats. Today, the sheer volume and concentration of data and digital transactions, coupled with easy global access throughout the business ecosystem, magnifies exposure to cyber attack.

The reward of a successful attack and the ability to remain anonymous and undetected presents an opportunity for anyone with a computer and Internet connection to infiltrate the business ecosystem. Cyber breaches damage reputations and destroy trust – both are vital ingredients for success in the digital age.

Organisations must establish a capability to provide continual insight and intelligence on the cyber threats facing the business. Armed with this insight, business leaders can anticipate and react dynamically to changes in their cyber threat profile.

Adversary	Motives	Targets	Impact
Nation state 	<ul style="list-style-type: none"> Economic, political, and/or military advantage 	<ul style="list-style-type: none"> Trade secrets Sensitive business information Emerging technologies Critical infrastructure 	<ul style="list-style-type: none"> Loss of competitive advantage Disruption to critical infrastructure
Organised crime 	<ul style="list-style-type: none"> Immediate financial gain Collect information for future financial gains 	<ul style="list-style-type: none"> Financial/payment systems Personally identifiable information Payment card information Protected health information 	<ul style="list-style-type: none"> Costly regulatory inquiries and penalties Consumer and shareholder lawsuits Loss of consumer confidence Financial loss
Hacktivists 	<ul style="list-style-type: none"> Influence political and/or social change Pressure business to change their practices 	<ul style="list-style-type: none"> Corporate secrets Sensitive business information Information related to key executives, employees, customers and business partners 	<ul style="list-style-type: none"> Disruption of business activities Brand and reputation Loss of consumer confidence
Insiders 	<ul style="list-style-type: none"> Personal advantage, monetary gain Professional revenge Patriotism 	<ul style="list-style-type: none"> Sales, deals, market strategies Corporate secrets, IP, R&D Business operations Personnel information 	<ul style="list-style-type: none"> Trade secret disclosure Operational disruption Brand and reputation National security impact

Adapting your cyber security approach

	Traditional information security approach	Cyber security approach
Scope of the challenge	<ul style="list-style-type: none"> Limited to the 'four walls' and the extended enterprise 	<ul style="list-style-type: none"> Spans your whole business ecosystem
Ownership and accountability	<ul style="list-style-type: none"> IT led and operated 	<ul style="list-style-type: none"> Business-aligned and owned; CEO and board accountable
Cyber threat characteristics	<ul style="list-style-type: none"> One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain 	<ul style="list-style-type: none"> Organised, funded and targeted; motivated by economic, monetary and political gain
Asset protection	<ul style="list-style-type: none"> One-size-fits-all approach – focused on data 	<ul style="list-style-type: none"> Prioritise and protect the data, transactions and operations that are most important to your business strategy
Defence posture	<ul style="list-style-type: none"> Protect the perimeter; respond if Attacked 	<ul style="list-style-type: none"> Plan, monitor, and rapidly respond when attacked
Security intelligence and information sharing	<ul style="list-style-type: none"> Keep to yourself 	<ul style="list-style-type: none"> Public/private partnerships; collaboration with industry working groups Be prepared for regulatory requirement to report breaches

Gaining advantage

Boards and executives that keep a sustained focus on cyber security do more than protect their business; they enable growth in the digital age.

All activities and investments are driven by the best available knowledge about information assets, threats, and vulnerabilities, and are evaluated within the context of business activity.

There are three areas we think you should consider when assessing your cyber security posture:

- Enhance your cyber security strategy and capability
- Understand and adapt to changes in the security risk environment
- Advance your security posture through a shared vision and culture

Cyber security at the heart of your business

Cyber security isn't just about technology. It also involves people, information, systems, processes, culture and physical surroundings. It aims to create a secure environment where businesses can remain resilient in the event of an attack.

Below are the six confidences that will help you to apply cyber security to the heart of your business.



People

Confidence in your people

Your people make critical security decisions every day.

Disappearing organisational boundaries mean that you can no longer rely on technology alone. You need to make sure your people understand security and act securely.

We can help you foster secure behaviours by shaping your culture and designing processes, systems and roles with human vulnerability in mind.



Technology

Confidence in your technology

Technology underpins your business.

As your business changes so should your technology. While embracing the new, you still need to protect legacy technology and information against cyber threats.

We can help you understand the inherent risks of your technology and how to mitigate them.



Connections

Confidence in your connections

Organisations exist in an increasingly complex digital ecosystem.

We share information and transact digitally more than ever before. Your digital relationships with customers, suppliers and others expose you to new areas of risk which need to be managed.

We can help you assess your connections, negotiate robust contracts and build an agile risk management framework, adept at keeping pace as your collaborative networks evolve.



Risk

Confidence to take risks

Digital opportunities cannot be realised without managing the inherent risks.

Some risks are worth taking, but if you're struggling to manage the downside, you won't be able to take advantage of the upside.

We can help you consider your interactions within the digital world and assess where and how they impact your past, present and future.



Crisis

Confidence during a crisis

Cyber attacks are now commonplace.

Resilience means being able to react quickly and effectively when compromised. Being aware of and prepared for threats will help you prevent incidents and react to them quickly enough to reduce their impact, and prevent them becoming a crisis.

We can help you protect what's important, detect intruders, deal with the regulators and minimise your exposure when you are compromised.



Priorities

Confidence in your priorities

Addressing cyber threats helps you prioritise what matters most.

Being prepared for changes in the digital era will help you get your priorities straight. A 'cyber savvy' governance and management structure means you can prioritise opportunities and know where you can afford to take risks.

We can help you to recognise your key tangible and intangible assets and align your security strategy to your priorities.

Building confidence

We view cyber security through a series of interconnected lenses. This rounded approach is designed to provide you with confidence: in your people, technology and connections, how you manage risk, set priorities and respond to an incident or during a crisis. Our approach typically begins with an assessment of your current capability and a recommendation of areas for improvement. This will enable you to develop a cyber security strategy to build confidence in your digital future.

You can't secure everything

We help you set the right priorities.

- Enterprise security architecture
- Protect what matters
- Strategy, organisation and governance
- Threat intelligence



Priorities



Risk

Seize the advantage

We help you exploit digital opportunity with confidence.

- Digital trust is embedded in the strategy
- Privacy and cyber security legal compliance
- Risk management and risk appetite



Crisis

It's not if but when

We help you build an intelligence led defence, enabling rapid detection and containment.

- Continuity and resilience
- Crisis management
- Incident response and forensics
- Monitoring and detection



Connections

Their risk is your risk

We help you understand and manage risk in your interconnected business ecosystem.

- Digital channels
- Partner and supplier management
- Robust contracts



Technology



People

Fix the basics

We help you use technology to your advantage, deriving maximum return from your technology investments.

- Identity and access management
- Information technology, operations technology and consumer technology
- IT security hygiene
- Security intelligence and analytics

People matter

We help you build and maintain a secure culture, where people are aware of their critical security decisions.

- Insider threat management
- People and 'moments that matter'
- Security culture and awareness

Confidence in
your digital future

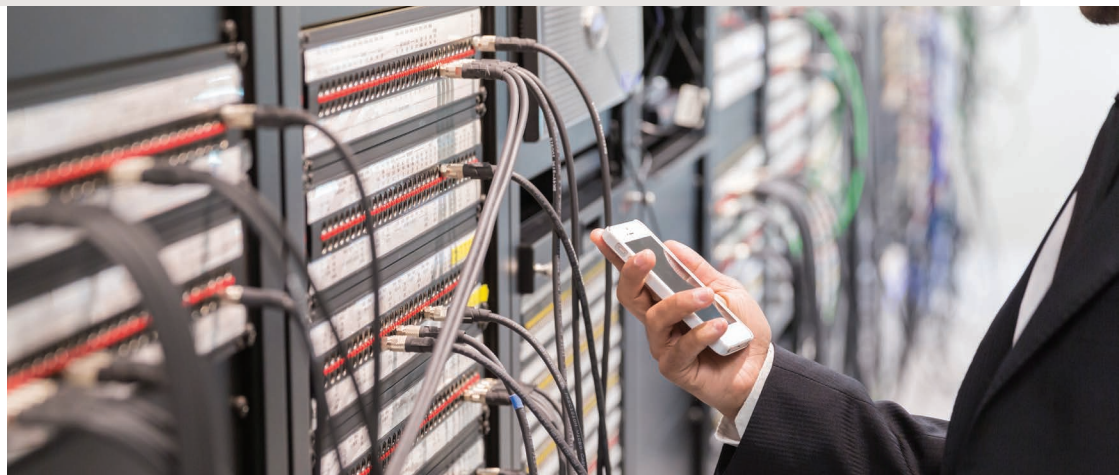
Cybersecurity services

Strategy & Transformation

Implementation & Operations

Incident & Threat Management

Privacy & Consumer Protection



Our services

We provide a comprehensive range of integrated cyber security services that help you assess, build and manage your cyber security capabilities, and respond to incidents and crises. Our services are designed to help you build confidence, understand your threats and vulnerabilities, and secure your environment. Our cyber security service delivery team includes incident response, legal, risk, technology and change management specialists.



Strategy & Transformation

Strategy Development & Redesign

- Risk Governance Strategy
- Security Policies, Standards and Procedures
- Security Awareness and Culture
- Business Continuity and Disaster Recovery

Cybersecurity Risk & Governance

- Cyber Security Risk Assessments
- Cyber Security Maturity Assessments
- Vulnerability Assessments

Third Party Risk Management

- Third Party Assurance
- Standardized Agreements
- Cloud providers



Implementation & Operations

Identity & Access Management

- Verifiable User Actions & Improved Customer Experience

Analytics & Monitoring

- Implement Security Data Analytics & Make Security Data Actionable

Data Protection

- Prevent Data Leakage and Exfiltration

Enterprise Security Architecture

- Architect a Secure Network
- Implement Secure Components



Incident & Threat Management

Incident Readiness

- Incident detection and response Assessment
- Technical penetration tests
- Real World Scenarios

Incident Response

- Incident Response Procedures
- Staff Training for first
- On-demand access
- Post-Incident analysis

Threat Intelligence & Information Sharing

- PwC's world-leading threat intelligence platform
- Intelligence Integration

Threat Management

- Threat Exposure
- Patching and updating schedules
- Secure Change Management and System Hardening



Privacy & Consumer Protection

Readiness Assessment

- Identify Privacy Related Processes
- Measure privacy risk

Implementation Roadmap & Support

- Roadmap Definition
- Privacy Controls

Data Registers & Flow Maps

- Data Registers
- Data Flows

Privacy Impact Assessments

- Privacy Impact Assessments
- Drive data protection decisions based on identified data privacy risks

DPO-as-a-Service

- Data Protection Officer
- Executive Privacy Decisions
- Advise on Privacy Matters

Contact us

Tassos Procopiou
Partner
Advisory
T: +357 - 22 555 750
tassos.procopiou@pwc.com

Dr. Iacovos Kirlappos
Manager
Advisory
T: +357 - 22 555 228
iacovos.a.kirlappos@pwc.com

PricewaterhouseCoopers Ltd

PwC Central, 43 Demostheni Severi Avenue, CY-1080 Nicosia
P O Box 21612, CY-1591 Nicosia, Cyprus
Tel: +357-22 555 000, Fax: +357-22 555 001



This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2019 PricewaterhouseCoopers Ltd. All rights reserved. PwC refers to the Cyprus member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.