

www.pwc.com/cybersecurity

CSOHIMSS Spring Conference

Cybersecurity and Privacy challenges in the Healthcare Ecosystem

May 2016

pwc

Objectives

1. Define Cybersecurity
2. Recognize the inherent vulnerabilities
3. How to operate in a new health ecosystem
4. Consideration for addressing the new reality

The new reality

The new reality...

Our perspectives

- Developed based on our interactions with CISOs, CIOs, CAEs, Corporate Suite Leadership, and Boards of Directors
- Shaped through knowledge and experience of developing strategies, implementing solutions and executing programs, and responding to security crises
- Supported and enhanced by years of healthcare industry, federal law enforcement, foreign intelligence and forensic experience
- Pragmatic insight and a balanced view of how to prioritize investments in people, processes and technology solutions needed to address the cybersecurity challenge
- Updated and refined based on healthcare industry trends, law enforcement alerts and key learnings from other industries (financial services, manufacturing and retail)

The new reality...

Highlights from PwC Global Information Security Survey

86%

Technology Advances

86% of Healthcare CEO's believe technological advances will transform their business

53%

Cyber Attacks a Serious Global Concern

53% of Healthcare CEO's are somewhat or extremely concerned by cyber attacks

283%

Financial Loss from Security Events

283% increase in the financial losses stemming from events in 2014, at an average of \$2.9M per organization

66%

Investing in Cybersecurity

66% increase in organization's investment in cybersecurity spending since 2013.

Sources:

- 1 - PwC 17th Annual Global CEO Survey
- 2 - PwC 6th Annual Digital IQ Survey
- 23- 2015 Global State of Information Security

The new reality...

What is cybersecurity?



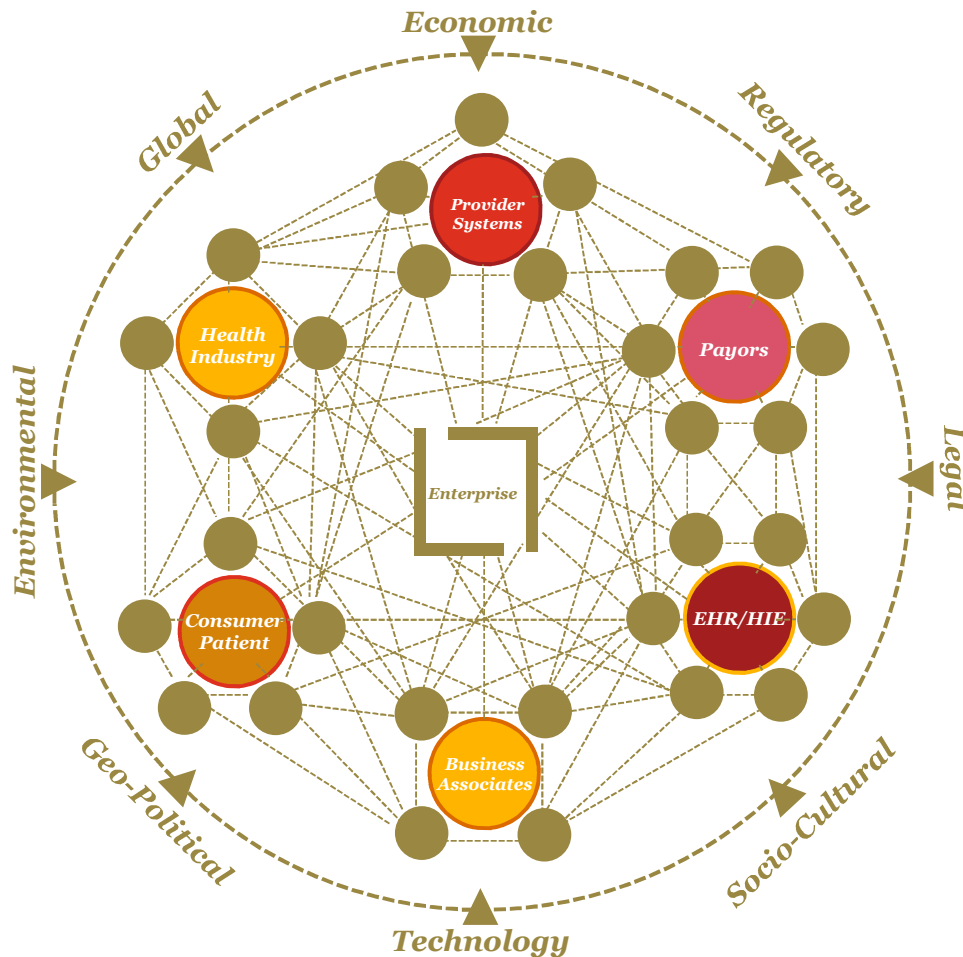
- Cybersecurity represents many things to many different people
- Key characteristics and attributes of cybersecurity:
 - **Broader** than just information technology and **extends** beyond the enterprise
 - **Increasingly vulnerable** due to technology connectivity and dependency
 - An ‘outside-in view’ of **the threats and business impact** facing an organization
 - Shared responsibility that requires **cross functional disciplines** in order to plan, protect, defend, react and respond

It is no longer just an IT challenge – it is a business imperative!

The new reality...

Beyond the enterprise

Health Ecosystem



▲ Pressures and changes which create opportunity and risk

The Evolution:

- Technology-led innovation has enabled business and care deliver models to evolve
- The extended enterprise has moved beyond technology and patient-provider integration
- Connectivity and collaboration now extends to all facets of business

Leading to:

- A dynamic environment that is increasingly interconnected, integrated, and interdependent
- Where changing business drivers create opportunity and risk

The new reality...

Technology domain convergence



Information Technology

Computing resources and connectivity for processing and managing data to support organizational functions and transactions such as user workstations, reporting repositories, data warehouses, web applications, etc.



Operational Technology

Systems and related automation assets for the purpose of monitoring and controlling physical processes and events or supporting the creation and delivery of products and services such as EHRs, nurse stations, hospital scheduling machines, drug allocation devices, etc.



Medical Devices

The healthcare industry includes a unique convergence of operational and consumer technology in the field of medical devices. These systems control physical processes and events supporting the delivery of medical services, while being external end-user focused, such as pacemakers, insulin pumps, CPAP machines, etc.



Consumer (Products and Services) Technology

Computing resources and connectivity integrated with or supporting external end-user focused products and services such as wearable medical devices, Health & Well-Being Rewards sites, etc.

Cybersecurity encompasses all *four* technology types

The new reality...

Threat actors and the information they target



Motives and **tactics** evolve and what adversaries target vary depending on the organization and the products and services they provide.

The new reality...

Why target healthcare?

1

Electronic Health Records are changing the information game

The healthcare business model has evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.

2

Health records are now worth more than credit cards and SSN

With Financial Services and Retail having long been targets for cyber attackers, the black markets are flooded with credit card and social security numbers, increasing the value of verified health records and identifiers for use in fraudulent access to healthcare as well as identity theft.

3

Healthcare, and new medical research, is a focus of developing nations' economic plans

Several developing nations have targeted existing healthcare technologies, including patient care and clinical improvements, and intellectual property for further "co-innovation" or "re-innovation" in order to jump start their national economic development plans.

4

Healthcare is less prepared to handle cyber events than FS and Retail


Traditional healthcare information security programs have long been narrowly-focused, compliance based efforts that have yet to adapt to the emerging and ever-changing threat landscape presented by these advanced threats.

5

Cybersecurity is seen as a barrier to patient care

Cybersecurity is not an just an IT issue; rather it requires attention and input from key business leaders, including executives, board or directors, legal, media relations, and others.

The new reality...
and adapting to it.

	Historical Perspective 	Today's Reality
Scope of the challenge	Limited to your “four walls” and the extended enterprise	Spans your interconnected global business ecosystem
Ownership and accountability	IT led and operated	Business-aligned and owned; CEO and Board accountable
Adversaries' characteristics	One-off and opportunistic; motivated by notoriety, technical challenge, and individual gain	Organized, funded and targeted; motivated by economic, monetary and political gain
Information asset protection	One-size-fits-all approach	Prioritize and protect your “crown jewels”
Defense posture	Protect the perimeter; respond if attacker	Plan, monitor, and rapidly respond when attacked
Security intelligence and information sharing	Keep to yourself	Public/private partnerships; collaboration with industry working groups

The shift is necessary because, healthcare data breaches today are less about accidental disclosure and more about targeted acquisition and unauthorized access to health records.

Events from the new reality

Events from the new reality...

Lessons learned from recent breaches in health industry demonstrate vulnerability and need to address core fundamentals...

- Attack Method - **organized and coordinated efforts** to use social engineering (phishing exploit), exploit Internet connectivity (fake infrastructure), and compromise system access (backdoor malware) for theft of business credentials
- Awareness - adversaries **tested and enhanced** their approach **over the course of months** before executing their campaign; intelligence sources communicated threat elements
- Detection - **technical indicators were undetected** during the attack sequence; additionally, as is often the case, third parties (e.g. law enforcement or the banks) detect the compromise first, **not** the company
- Security Posture - **known companies compromised** were assumed to be **compliant** with industry standards (e.g. HIPAA, PCI DSS) -- compliance does not equal security
- Industry Exposure – attacks are often **not limited to a single company**; many companies within an industry sector share the same / similar profile and it is highly likely there are other targets and victims

Events from the new reality...

Meeting the HIPAA Privacy and Security Rules may not be (is not) sufficient to prepare an organization for today's threats

- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is implemented by **covered entities and business associates** through adoption of the **HIPAA Privacy Rule** and the **HIPAA Security Rule**
- The HIPAA Privacy Rule – **only addresses** appropriate use and disclosure of protected **health information (PHI)** in physical or electronic form
- The HIPAA Security Rule – only addresses **administrative, physical, and technical safeguards for a subset of PHI** that is created, received, maintained, or transmitted, in **electronic form (ePHI)**
- Limitations of scope
 - **Data** - other types of critical data, for example, **intellectual property, authentication credentials, or non-public financial information**, are **not** necessarily protected, even if an organization meets the HIPAA rules
 - **Threats & Vulnerabilities** – requirements **do not** specifically **address evolving threats and vulnerabilities**, and as such, the required Security Rule controls only provide a baseline for implementing safeguards and do not specifically address Advanced Persistent Threats and the evolving threat landscape.
- But, HIPAA Risk Assessments, done properly, can provide insight regarding the threats and vulnerabilities that relate to the risk surrounding PHI for a covered-entity or business associate.

Events from the new reality...

Once a security and compliance activity, incident response is now a board level and audit committee issue

- The industry has faced regulatory scrutiny for data loss / breaches previously; however these cybersecurity attacks are significantly different in their objectives, execution and impact. For instance these new cyber attackers are:
 - Seeking PHI/PII data for resale on black market for fraudulent access to healthcare products and services (i.e. Medicare, which is not reimbursable)
 - Targeting intellectual property including clinical trial data for new pharmaceuticals
 - Utilizing sophisticated threat actors with exceptional technical skills and experience
 - Employ advanced persistent threats to avoid detection and propagate your network seeking valuable information including intellectual property, trade secrets, etc.
- While some companies are thinking about proactive actions and some will operate reactively; PwC belief is to lead your response with a **business impact based approach**

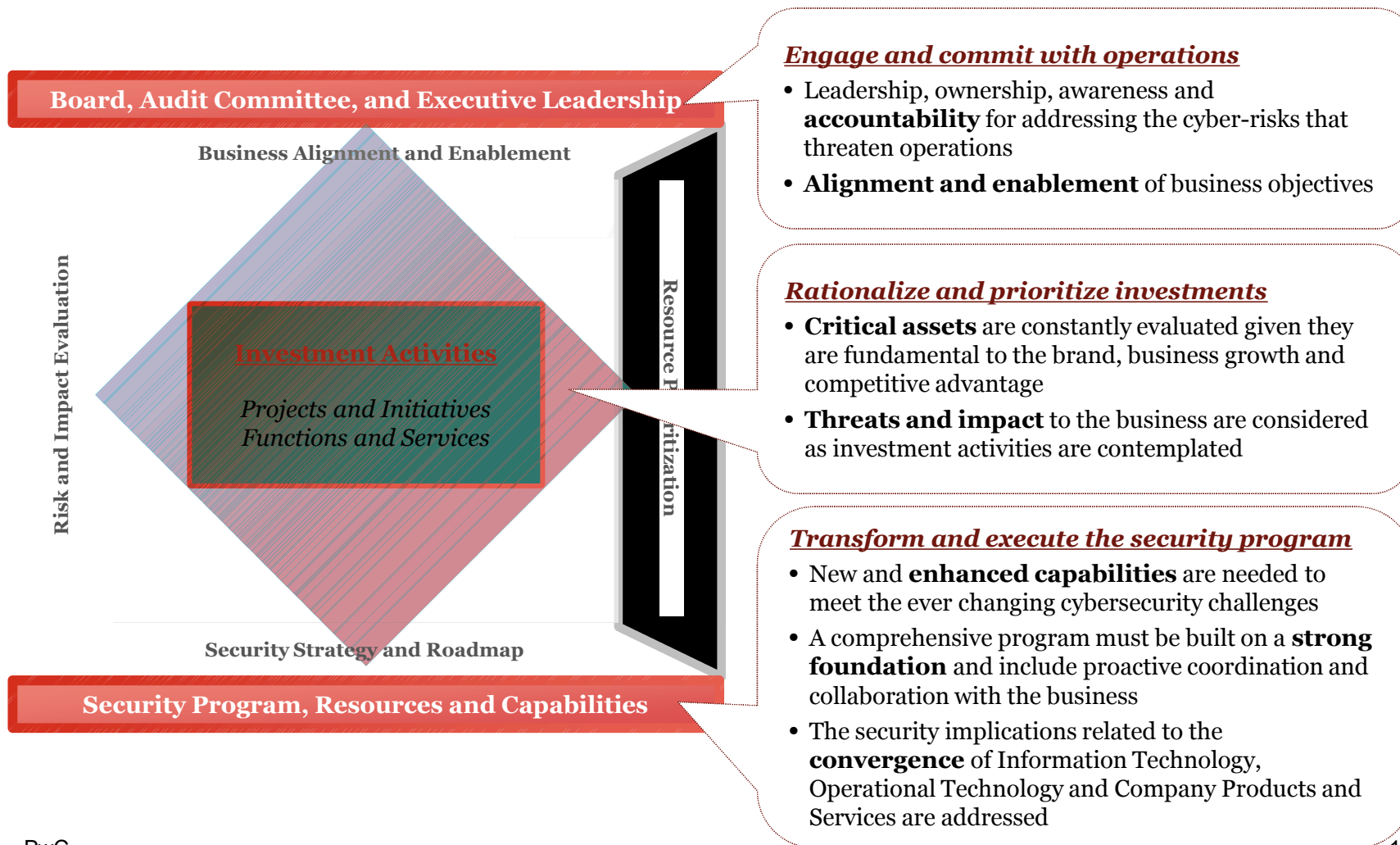
Risks

- **Financial:** fines, remediation, cost to defend
- **Reputational:** brand impact, loss of confidence
- **Operational:** inaccurate or unavailable data, systems, or devices
- **Regulatory:** active federal and state regulators, increasing enforcement
- **Legal:** lawsuits, class action
- **Compliance:** evolving domestic & international laws
- **Contractual:** compliance with “promises” made – yours and your vendors/third parties

Adapting to the new reality

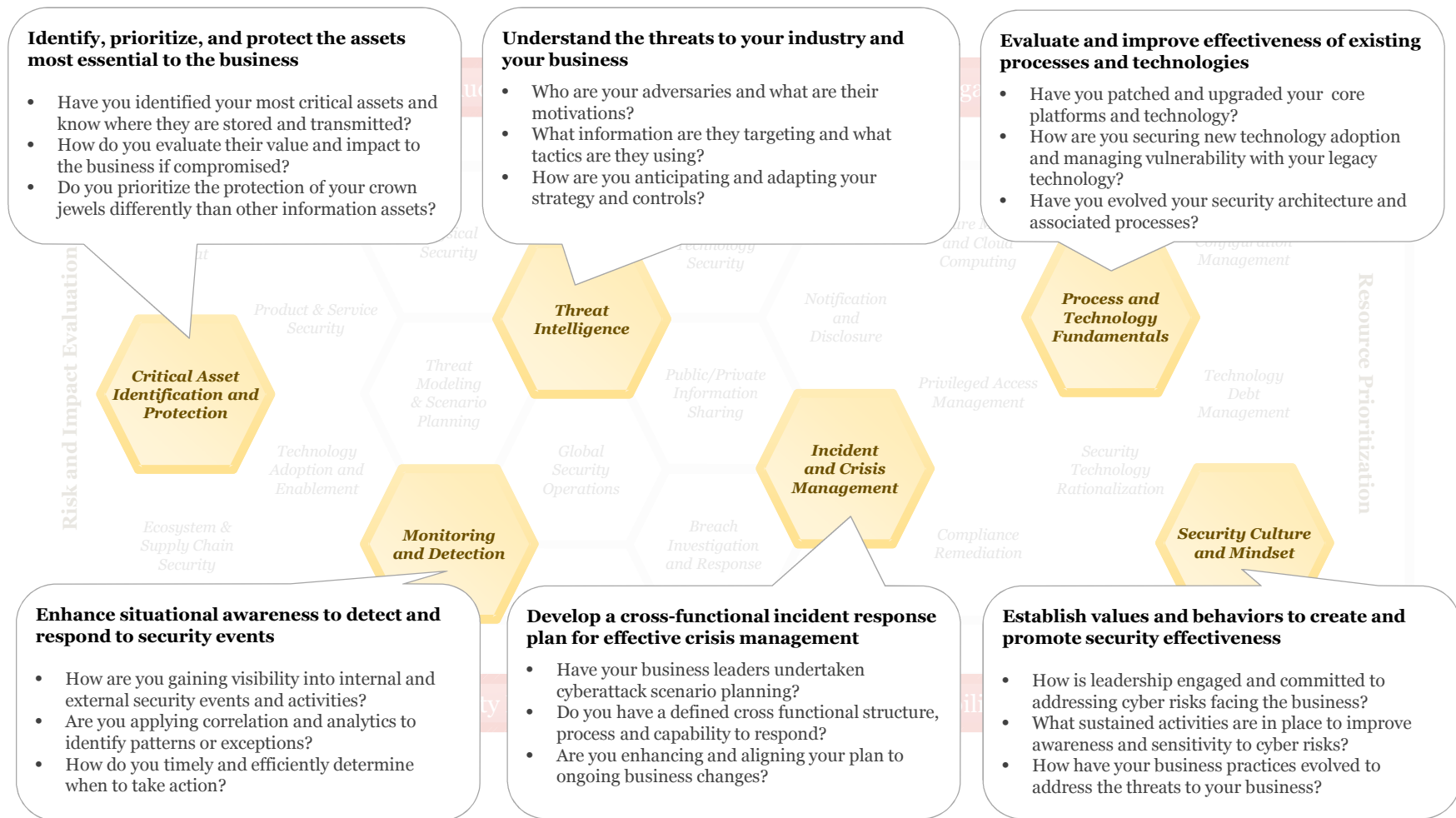
Adapting to the new reality...

Operating in the new health ecosystem requires you to think differently about your security program and investments.



Adapting to the new reality...

Questions to consider when evaluating your ability to respond to the new challenges.



Adapting to the new reality...

Key points to consider

1

The global business ecosystem has changed the risk landscape

Business models have evolved, creating a dynamic environment that is increasingly interconnected, integrated, and interdependent - necessitating the transformation of your security practices to keep pace.

2

Focus on securing high value information and protecting what matters most

Rather than treating everything equally, you should identify and enhance the protection of your “crown jewels” while maintaining a consistent security baseline within their environment.

3

Know your adversary – motives, means, and methods

Sophisticated adversaries are actively exploiting cyber weaknesses in the business ecosystem for economic, monetary or political gain – requiring threat intelligence, proactive monitoring and deep response capabilities.

4

Embed cybersecurity into board oversight and executive-level decision making

Creating an integrated, business aligned security strategy and program requires awareness and commitment from the highest executive levels of the organization – in order to apply the appropriate resources and investments.

Adapting to the new reality... **Questions Boards and CEO's should be asking**

<p><i>Enhancing their cybersecurity strategy and capability</i></p>	<ol style="list-style-type: none"> 1. Is our cybersecurity program aligned with our operational strategy? 2. Do we have the capabilities to identify and advise on strategic threats and adversaries targeting us? 3. Can we explain our cybersecurity strategy to our stakeholders? Our patients? Our investors? Our regulators? Our ecosystem partners?
<p><i>Understanding and adapting to changes in the cybersecurity risk environment</i></p>	<ol style="list-style-type: none"> 1. Do we know what information is most valuable us? Our providers? Our patients? 2. Do we know what our adversaries are after / what would they target? 3. Do we have an insider threat program? Is it inter-departmental? 4. Are we actively involved in relevant public-private partnerships? Information sharing?
<p><i>Advance their cybersecurity posture through a shared vision and culture</i></p>	<ol style="list-style-type: none"> 1. How was our last security crisis identified; in-house or government identified? 2. Who leads our incident and crisis management program? Is our program cross functional / inter-departmental? 3. How often are we briefed on our cyber initiatives? Do we understand the cyber risks associated with certain business decisions and related activities? 4. Have we made investments into prevention? Response? Resilience?

Addressing the new reality

Strategic steps to address cybersecurity risks

Organizations can't eliminate the risk of cyber attacks, but they can minimize their consequences. Here are 5 things leading organizations do to combat cybersecurity risks.



Tactical Information Security actions to consider

Here are 4 actions to consider in the short term to determine the current state of your environment and cybersecurity program.

-  ***Establish on-call incident response agreement(s) with forensic experts and outside counsel.***
-  ***Conduct a Breach Indicator Assessment and Threat Model to determine “Are you compromised and don’t know it?”***
-  ***Perform a gap analysis and security risk assessment to determine your cybersecurity program’s current maturity.***
-  ***Review your cybersecurity program strategy and incident readiness at the Board level.***

Tactical Internal Audit actions to consider

Perform a cybersecurity audit

- To gain an understanding of the current state and maturity of the information security (IS) and privacy programs.
- Identify information security and privacy risks and gaps using a chosen framework (NIST, ISO, HITRUST, PwC).
- Provide recommendations for enhancement and improvement.

Scope of Audit

- Assess the current state information security and privacy programs across relevant processes and systems,
- Identify potential risks and process gaps based on review of policies and procedures and program governance, and
- Provide a current state maturity level with recommended enhancements to improve the information security and privacy programs.

Assessment Elements

- Process to identify, assess, and mitigate security threats and vulnerabilities.
- The capture, processing, storage, and distribution of data and information.
- Alignment and incorporation of operational domains within information security and privacy programs.
- Correlation of information security and privacy programs to strategic and operational IT and business objectives.
- Consideration and integration of identified future information security and privacy initiatives within the security organization and privacy & compliance teams.

For more information on cybersecurity...



www.pwc.com/cybersecurity

- [10Minutes on the stark realities of cybersecurity](#)
- [Answering your Cybersecurity Questions](#)
- [2014 US State of Cybercrime Survey Whitepaper](#)
- [Why you should adopt the NIST cybersecurity framework](#)
- [Results of 2015 Global State of Information Security](#)
- [Cybersecurity risk on the board's agenda](#)
- [A response to the President's Cybersecurity Executive Order](#)
- [Cyber Video Series](#)