www.pwc.com

Cybersecurity and Privacy Hot Topics 2015

pwc

Table of Contents

Cybersecurity and Privacy Incidents are on the rise

Executives and Boards are focused on Emerging Risks

Banking & Capital Markets – Sector Trends

Cybersecurity & Privacy Hot Topics

Achieving a Strategic Cybersecurity and Privacy Program

Cybersecurity and Privacy Incidents are on the rise

Today, cybersecurity and privacy compromises are a persistent—and globally pervasive—business risk

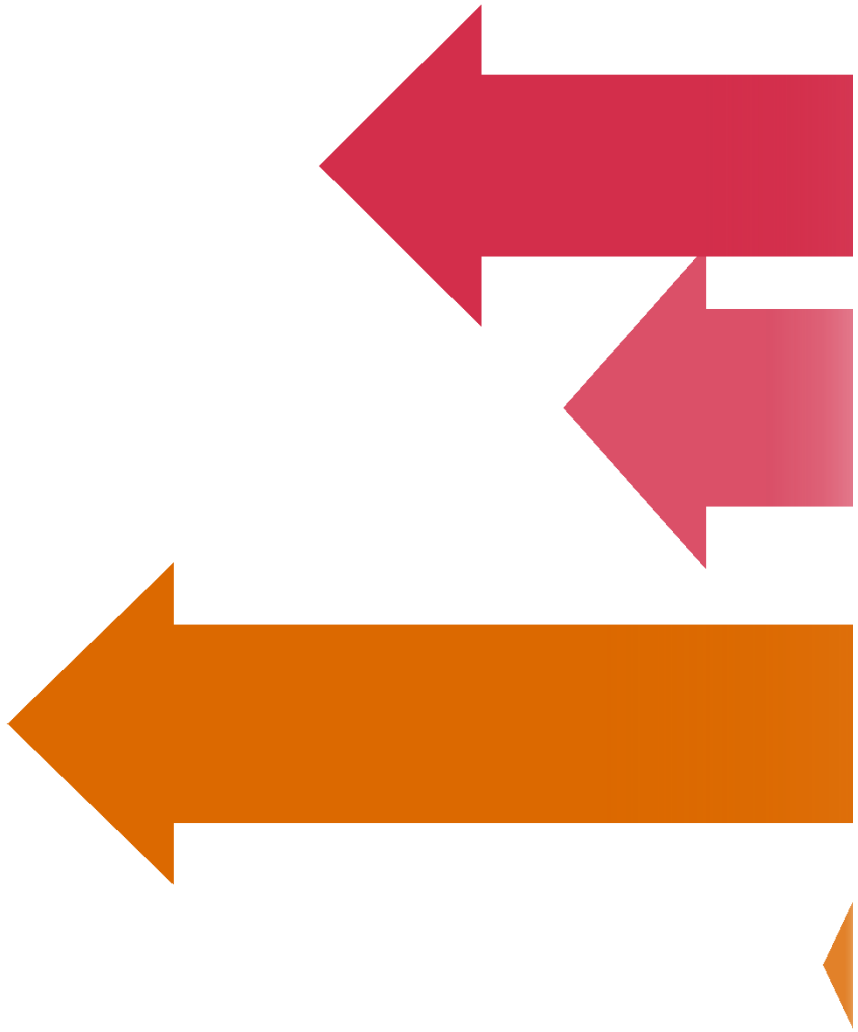
- The US government notifies **3,000 companies** that they were attacked and charged nation-backed hackers with economic espionage.
- Compromises of retailers culminate in a recent breach of **56 million credit cards**.
- A number of recent **data breaches** reported by large financial institutions and retailers.
- Powerful malware **infects hundreds of energy companies** worldwide.
- More than half of **global securities exchanges** are hacked.
- **Regulators around the world** are beginning to more proactively address cyber risks.

The financial cost of incidents is high and rising

As cybersecurity incidents grow in frequency, the costs of managing and mitigating breaches also are rising.

Globally, the annual estimated reported average financial loss attributed to cybersecurity incidents was **$2.7 million**, a jump of 34% over 2013.

Not surprising, but certainly attention grabbing, is the finding that big losses are more common: Organizations reporting financial hits of $20 million or more **increased 92%** over 2013.



Incidents attributed to insiders rises while security preparedness falls

Current and **former employees** are the most-cited culprits of security incidents, but implementation of key insider-threat safeguards is declining.

• 56% have privileged user-access tools (65% in 2013).

• 51% monitor user compliance with security policies (58% last year).

• 51% have an employee security training and awareness program (60% in 2013).

Compromises attributed to **third parties with trusted access** increases while due diligence weakens.

• 55% have security baselines for external partners, suppliers, and vendors (60% in 2013).

• 50% perform risk assessments on third-party vendors (53% in 2013).

Executives and Boards are focused on Emerging Risks

CEOs/Boards are no longer ignoring cybersecurity and privacy issues

Cybersecurity and privacy is an enterprise-wide issue:

- Increase in the security and privacy **regulatory mandates** in recent years, as well as expected changes in upcoming years.
- Boards are no longer willing to accept the risk that technology can pose to the business.
- **Emerging technologies** and reliance on **third parties** have created a borderless infrastructure resulting in increased exposure.
- Growing **demand by business leaders** to understand how to protect the data deemed sensitive.
- **Increase in threats and vulnerabilities** to sensitive data and corporate assets.
- Businesses continue to struggle to maintain accountability to their stakeholders and establish effective strategies and standards for security risk management.

Cybersecurity & privacy are business issues

Why cyber threats have become business risks

Put security on your agenda before it becomes an agenda

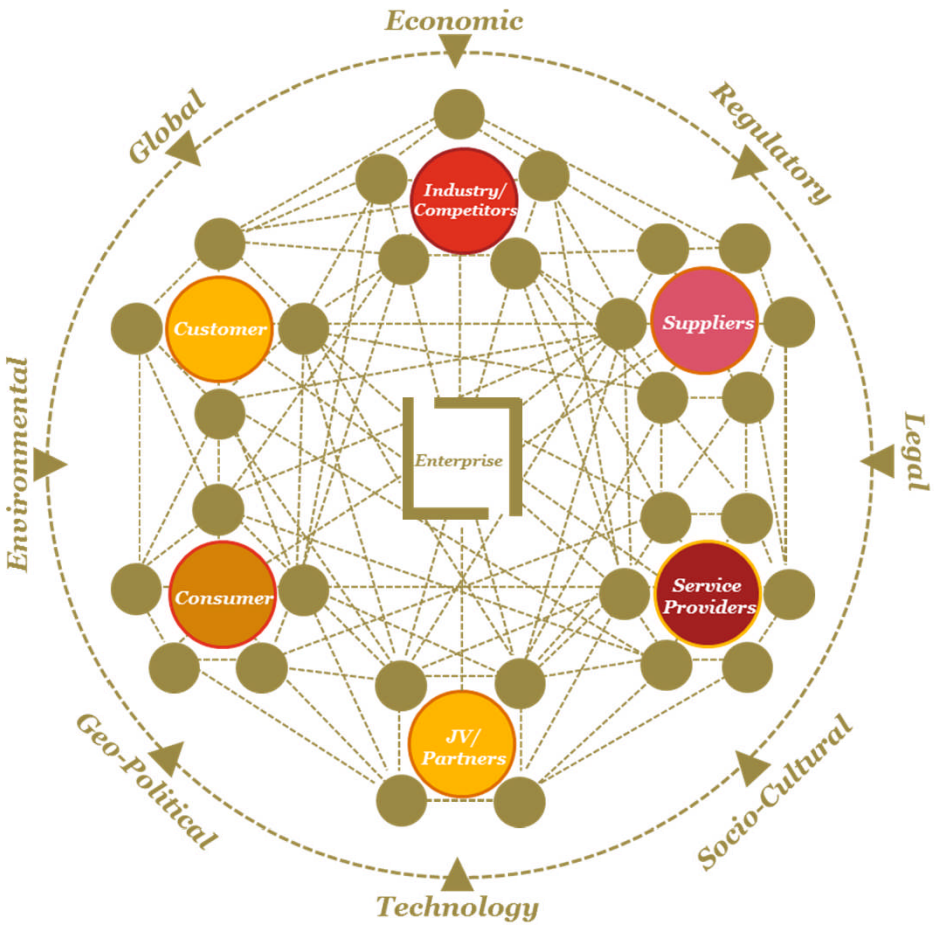
Who's behind this massive loss of data?

Compliance does not equal security or does it?

Do you think the implementation of tools is fool proof security?

The cybersecurity and privacy challenge now extends beyond the enterprise

Global Business Ecosystem



▲ *Pressures and changes which create opportunity and risk*

Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly interconnected, integrated, and interdependent.

- The ecosystem is **built around a model of open collaboration and trust**
- Constant **information flow is the lifeblood of the business ecosystem**. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- **Adversaries are actively targeting critical assets** throughout the ecosystem—significantly increasing the exposure and impact to businesses.

Banking & Capital Markets – Sector Trends

Banking & Capital Markets Sector Trends and Focus Areas

- Increase in the number as well as oversight of both domestic & global regulations.
- While organizations have made significant security improvements, they have not kept pace with today's determined adversaries – many rely on yesterday's security practices to combat today's threats.
- Use of complex, rapidly evolving, and sophisticated technologies pose a "significant challenge" for the future success of an organization's information security.
- The average number of annual detected incidents has increased, evidencing today's elevated threat environment. As a result, total financial losses due to incidents has risen given the cost and complexity of responding to threats.
- Mobile security is an area of continued vulnerability. Mobility has generated a deluge of business data, but deployment of mobile security has not kept pace.
- While attacks backed by nation-states make headlines, Banking & Capital Market firms are more often targeted by hackers and organized crime.
- Companies are increasingly sharing data with third parties. While services can be outsourced, accountability for security cannot. Many organizations do not include provisions for cloud services in their security policies.

Key Cybersecurity Risks – Banking & Capital Markets

- Damage to brand & reputation – loss of share value, loss of market confidence
- Financial and intellectual property– loss of credit, cash, competitive edge, trading algorithms and techniques
- System inoperability caused by a breach – inability to execute trades, access to information

On Nov 3rd 2014 – FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center.

Reference Link - *https://www.ffiec.gov/press/pr110314.htm*

On Dec 10th 2014 - NY DFS announced - "DFS-regulated Banks to be examined based on cyber security protocols, governance, third-party vendor IT security, and other issues. Also targeted cybersecurity assessments will be integrated as ongoing, regular part of DFS exam process."

Reference Link *- http://www.dfs.ny.gov/about/press2014/pr1412101.htm*

Metrics that Matter*
The cost of security incidents jumped 24% with big losses leading the way. The number of financial firms reporting losses of $10 million to $19.9 million increased by a head-turning 141% over last year.

* Source: PwC's 2015 Global State of Information Security Survey.

SEC Cybersecurity Preparedness Exam

- On April 15th 2014, the SEC had announced the Office of Compliance Inspections and Examinations (OCIE) will audit more than 50 registered broker-dealers and investment advisers for cybersecurity preparedness.

- **On Feb 3rd 2015**, the OCIE issued a Risk Alert that provides summary observations from OCIE's examinations of registered broker-dealers and investment advisers, conducted under the Cybersecurity Examination Initiative.

  - ✓ OCIE's National Examination Program staff examined 57 registered broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with cybersecurity.
  - ✓ The examined firms were selected to provide perspectives from a cross-section of the financial services industry and to assess various firms' vulnerability to cyber-attacks.

Reference Link http://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

Evolving perspectives

Considerations for businesses adapting to the new reality

	Historical IT Security Perspectives	Today's Leading Cybersecurity Insights
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* attacked	• Plan, monitor, and rapidly respond *when* attacked
Security intelligence and information sharing	• Keep to yourself	• Public/private **partnerships**; collaboration with **industry working groups**

Motivated Adversaries

...what are your most valuable information assets, and what are your adversaries after? Protection of these assets must be prioritized.

Adversary	Motives	Targets	Impact
Nation State	• Economic, political and /or military advantage	• Trade secrets • Sensitive business information • Emerging technologies • Critical infrastructure	• Loss of competitive advantage • Disruption to critical infrastructure • Monetary loss
Organized Crime	• Illicit profit • Fraud • Identity theft	• Financial / Payment Systems • Data breaches and intellectual property theft • Third-party service providers	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
[redacted]			
[redacted]			

Data identification and classification is becoming more difficult

Key message

Are you protected against both internal and external data leakage? How can you adequately protect your data without knowing where it is?

Questions

- Do you have a complete **inventory of what sensitive data** you create and collect, where it's stored, who has access to it, and how it's used?
- Do you have **data flow maps** to understand how data moves within and outside of your organization?
- Do you **collect, process, store, transmit, use, or dispose** of personally identifiable data of individuals originating from the US or **outside of the US**? Is this data transferred across national borders?
- Do you collect, process, store, transmit, use, or dispose of **protected health information**?
- Do you **share** personally identifiable data **with third parties** including cloud providers and if so, do you know what data is transferred or disclosed to each third party? Who owns this data once shared?
- How do you **monitor data use** across all platforms (internal and external) in accordance with policy?

Digital convergence brings new challenges and extends beyond the enterprise

1980's

- IT, OT and CT operate in different environments and on different platforms
- OT and CT are based on proprietary platforms
- Data is not shared between technologies
- OT and CT face little to no cyber risk since they are not connected to a network

1990's

- OT is networked to allow centralized operation
- CT remains in a separate environment
- OT becomes vulnerable due to the connection, but is partially protected by the obscurity of proprietary solutions

2000's

- OT connects to IT using standardized IT channels to reduce costs and increase compatibility
- Boundaries between IT and OT start to blur
- CT connects to IT through pur- pose built channels
- OT is no longer protected by obscurity and CT is now vulnerable. Traditional IT security does not cover either

2010's

- The technology underlying IT has become ubiquitous across OT and CT
- The combination of these three represents the integrated technology ecosystem
- IT, OT and CT are all vulnerable to cyber threats. Businesses must adapt their security model to include the full scope of technologies

Information Technology

Operational Technology

Consumer Technology

Internet

Proprietary Connection

IT Protocol Based Connection

Cybersecurity & Privacy Hot Topics

Cybersecurity & Privacy Topical Issues: Balancing Business Enablers vs Business Risks

Organizational Structure & Talent Strategy

Security organizations have often grown organically with the growing risk. We need to take a step back to assess whether our structure is sufficient to deliver a meaningful information security strategy.

Transferring Data Across International Borders

Managing cross border clearance in the face of ever-changing regulatory requirements can be a daunting task.

Incident Response

While breaches and incidents continue to rise, organizations need to focus on creating a comprehensive Incident Response Management Program.

Threat Intelligence &Vulnerability Management

Keeping up with the attackers and connecting with others to enhance threat intelligence is an uphill battle.

Mobility & Social Media

Mobile devices, mobile applications, social media, and accelerated product life cycles are just the latest contributors to risk of an enterprise.

Cybersecurity & Privacy as a Competitive Advantage in the Marketplace

Organizations are beginning to leverage their security and privacy programs as market competitive advantages through the issuance of SOC 2 and other consumer facing reports

Cybersecurity & Privacy Topical Issues: Balancing Business Enablers vs Business Risks

Insider Threats

Organizations need to focus on the insider threat along with the cyber threat.

Adaptive Security Architecture

Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.

Sensitive Data Discovery

Recent high-profile data loss incidents have increased scrutiny on management to identify, categorize and appropriately secure data.

Engaging with the Boards

Obtaining board level and executive level support for security/privacy initiatives is imperative for an organization to maintain an effective security program.

Digital Convergence (OT, IT, CT)

The technology underlying IT has become ubiquitous across OT and CT. IT, OT and CT are all vulnerable to cyber threats. Businesses must adapt their security model to include the full scope of technologies.

Third Party Vendors & Cloud Computing

While risks associated with third parties and cloud computing continue to increase, many companies are less prepared to defend their data.

Achieving a Strategic Cybersecurity & Privacy Program

Taking action: steps toward a strategic security program

1. Determine the organization's current security posture and capabilities and compare these results with organizations of similar size/complexity/industry
2. Develop a Roadmap to migrate the organization from the current environment to the future state environment
3. Identify your most valuable information assets, and prioritize protection of this high-value data
4. Understand your adversaries, including their motives, resources, and methods of attack to help reduce the time from detect to respond
5. Assess cybersecurity/privacy risks of third parties and supply chain partners, and ensure they adhere to your security/privacy policies and practices
6. Collaborate with others to increase awareness of cybersecurity/privacy threats and response tactics

Information security & privacy program components

Strategy and Governance

- Prioritize investments, allocate resources, and align security and privacy capabilities with the Strategic imperatives and initiatives of the organization.
- Develop policies, procedures, and standards

Training and Awareness

- Comprehensive training with defined elements, audience, frequency and sanctions
- Monitoring of training completion

Risk & Compliance Assessment

- Risk Assessment
- Applicable laws and regulations
- Business process risk ranking
- Data flow mapping and inventory
- Privacy & security impact assessment

Framework of Control

- Enforce Policies & Procedures
- Security Architecture & Services
- Threat Intelligence & Vulnerability Management
- Identity & Access Management
- System Resiliency
- Privacy by design
- Notice, choice, consent, use controls
- Third Party Risk Management

Monitoring and Auditing

- Periodic testing of control effectiveness
- Independent assessments

Incident Identification & Response

- Identify Incidents
- Assess risk
- Prioritize response
- Defined response and breach notification plan
- Testing of plan
- Inclusion of third party

How we can help?

Overall Program Assessments

- Program maturity/strategy assessments
- Governance Reviews
- Design/implementation of a sustainable program
- Internal audit assessments
- Compliance reviews
- Data Inventories
- Third party/vendor risk analysis
- Incident response plans reviews
- AT101 & SOC 2 (Privacy, Security, Confidentiality)

Privacy Specific Assessments

- ISO 27002 or GAPP reviews (enterprise-wide or application specific)
- Regulatory/attest readiness
- Regulatory/attest reporting

Security Specific Assessments

- Technical Security Assessments/Audits
  - Infrastructure(Operating Systems, Databases, Network)
  - Mobile Device Management (Phone, Tablet)
- Threat & Vulnerability Management
  - Attack & Penetration Testing (Ethical Hacking)
  - Server Vulnerability Assessment
- Business Continuity/Disaster Recovery / Social Media (Spear Phishing) Assessment

Cybersecurity & Privacy

Dave Roath
Partner, Cybersecurity & Privacy
(646) 471-5876
david.roath@us.pwc.com

Abhishek Bharti
Cybersecurity & Privacy
(646) 471-4708
a.bharti@us.pwc.com