www.pwc.com

Cyber Crime Conference

Risk Management in a Cyber Era

Strictly Private and Confidential

June 18 2013

pwc

Angreb på NemID bekymrer

Lørdag d. 13. apr. 2013 kl. 23:16 af Henrik Rewes / here@tv2.dk

Foto: TV 2

31 1 0 0 0

PRINT ARTIKEL

SEND TIL EN VEN

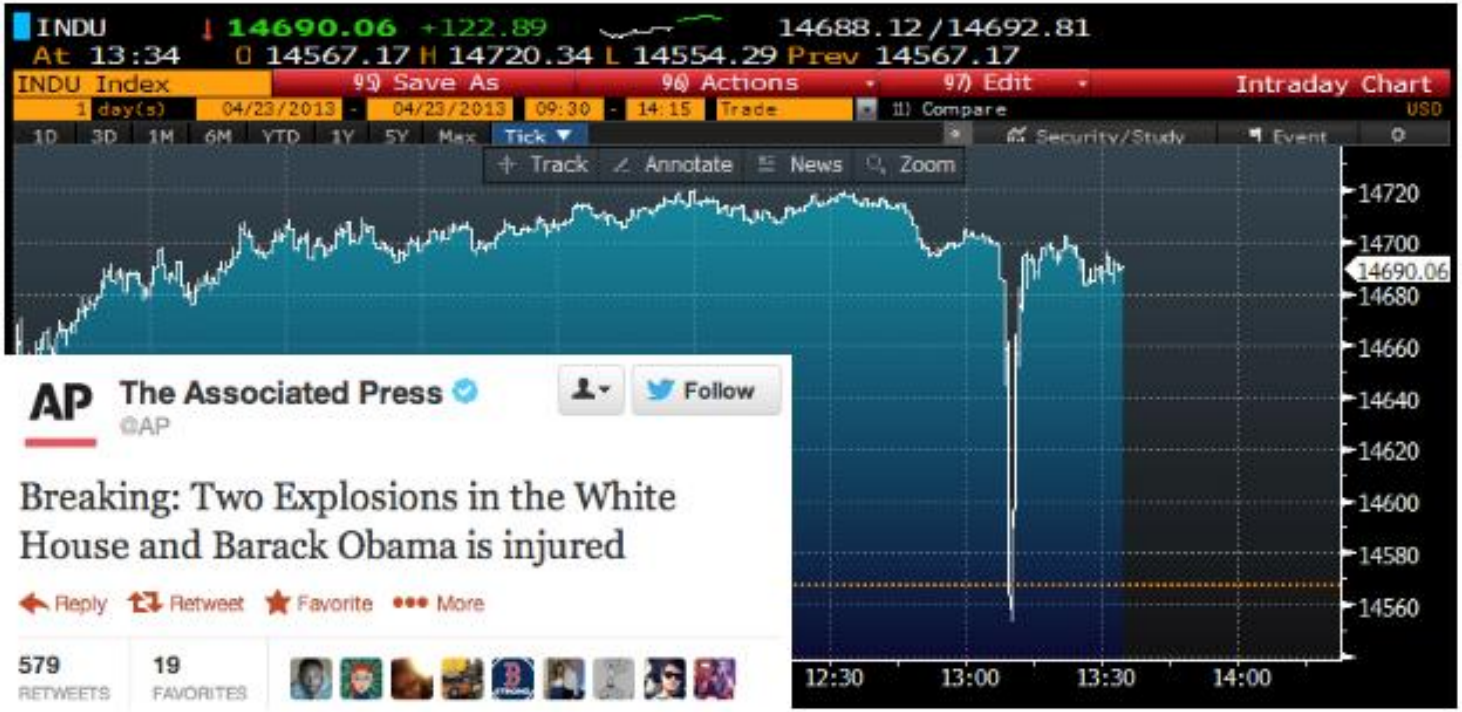
Det vellykkede hackerangreb på NemID torsdag skaber bekymring i Beredskabsstyrelsen. Styrelsen har det overordnede ansvar for, at Danmark er forberedt på de katastrofer, der kan ramme landet.

The Washington Post

Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?

By Max Fisher, Published: April 23, 2013 at 4:31 pm E-mail the writer

2 Comments | Like 135 | Tweet 37 | More



version2

IT-NYHEDER ... HITEPAPERS

EMNER Cy...

Se kommentarer (1)

Berec...andt de ti største...

I en ny risiko...-10-listen. Truslen skal ...

Af Jesper Kildebo...

Et cyberangreb m... ammen med gamle kendinge s... vurderer Beredskabsstyrelse... netop er udkommet. Det er første gang, Beredsk... rten og top-10-listen.

News

Cyber risk now in the top five global risks

13 January 2012

Last year's report from the World Economic Forum placed cyber security as 'a risk to watch'. This year's study, the World Economic Forum Global Risks 2012, has elevated that to one of the top five actual risks.

Why is Cybercrime interesting for PwC?

We are a global consulting firm with more than 8,000 security practitioners around the world

In Denmark, we help public and private organizations with implementing and testing technology and provide wide variety of security consulting services:

- Secure architecture
- Security in the development lifecycle
- Risk-based penetration testing
- Forensics services
- Maturity and benchmarking assessments
- Business impact assessments
- Cyber-simulation scenarios

Who am I?

Christian Kjaer

Director – information & cyber security

Cand.merc.

CISM, CISSP, ESL

PwC

Protego

VIGILANTe

idata international

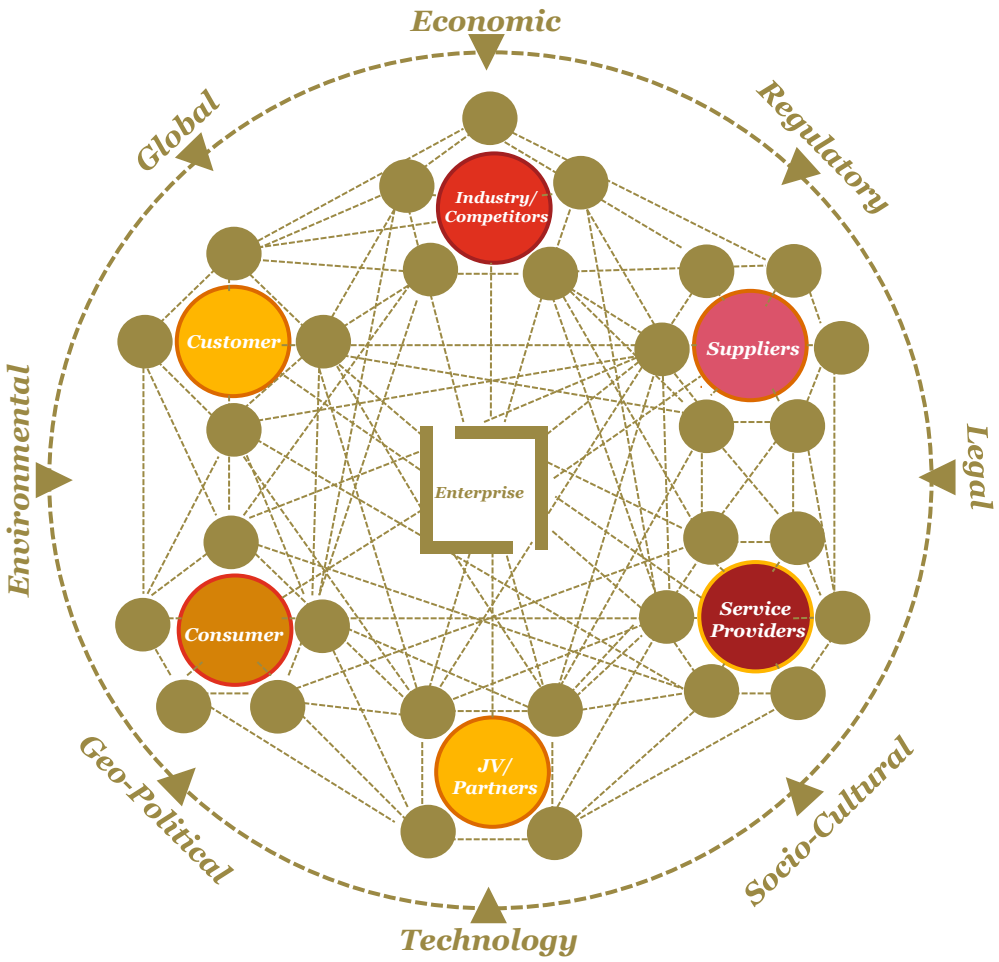
The new reality

- New technologies, well-funded and determined adversaries, and interconnected business ecosystems have combined to increase your exposure to cyber attacks.
- Critical digital assets are being targeted and the potential impact to organizations has never been greater.
- In order to sufficiently protect the business, future cash flows, and shareholder value, the approach to cyber security must keep pace.
- Business that are successfully adapting to the new reality are doing more than protecting the business; they are reaping bottom line benefits.

How businesses are 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
	•	•
	•	•
	•	•
	•	•
	•	•

Your business ecosystem creates both opportunity and risk



- Increase in technology reliance
- Built on trust and collaboration
- Information and data ubiquity throughout

- New and advanced adversaries take advantage of the above characteristics

How businesses are 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
	•	•
	•	•
	•	•
	•	•

How businesses are 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
	•	•
	•	•
	•	•

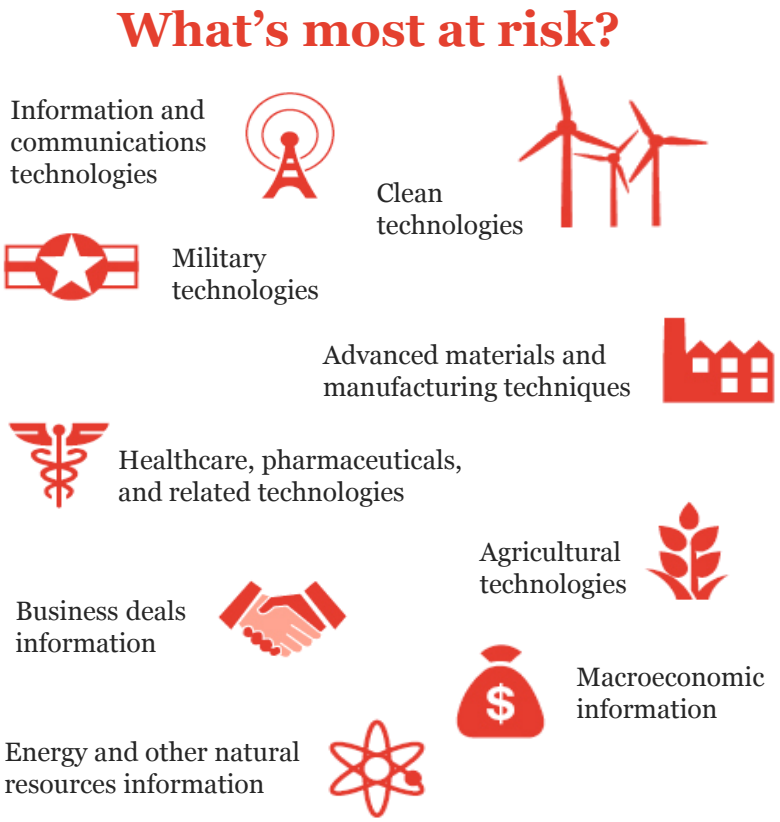
Why cyberthreats have become business risks

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
Organized Crime	• Immediate financial gain • Collect information for future financial gains	• Financial / payment systems • Personally Identifiable Information • Payment Card Information • Protected Health Information	• Costly regulatory inquiries and penalties • Consumer and shareholder lawsuits • Loss of consumer confidence
Hacktivists	• Influence political and /or social change • Pressure business to change their practices	• Corporate secrets • Sensitive business information • Information related to key executives, employees, customers & business partners	• Disruption of business activities • Brand and reputation • Loss of consumer confidence
...and even			
Cyber Terrorists	• Political and/or ideological change • Create fear, uncertainty, and doubt	• Critical infrastructure • Operational technologies • Highly visible venues	• Destabilize, disrupt, and destroy physical and logical assets

How businesses are 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"
	•	•
	•	•

What information really matters—to your business and your adversaries?



Source: Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.*

- Business executives should understand what their most valuable information assets are and where they are located in the business ecosystem at any given time
- Businesses should prioritize and allocate resources to effectively protect the "crown jewels" today and into the future

How businesses are 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
	•	•

How businesses are 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

Three areas to initially consider when assessing your cybersecurity posture

Enhance your cybersecurity strategy and capability	Is an integrated cybersecurity strategy a pivotal part of our business model? Does the strategy consider the full scope of security: technical, physical, process, and human capital? Have we applied the required resources and investments? Do we have the security capability to advise internal business leaders on critical threats, emerging technology, and strategic initiatives? Can we explain our cybersecurity strategy to our stakeholders? Our investors? Our regulators? Our ecosystem partners?
Understand and adapt to changes in the security risk environment	Do we know what information is most valuable to the business? Have we prioritized security to protect those assets accordingly? Have we quantified the business impact if the assets were impaired? Do we understand the significant changes in the threats facing our business? Who are our adversaries? What would they target? What techniques might they use? Are we actively acquiring and adapting to internal and external sources of intelligence? How are our controls and countermeasures responsive to events and activities? Are we actively involved in relevant public-private partnerships?
Advance your security posture through a shared vision and culture	Does the chief information security officer role report, independent of IT, to the board or an executive leadership team committed to cybersecurity? Do employees understand their role in protecting information assets—have we provided the necessary tools and training? What assurances do we require from suppliers and service providers? Do we actively monitor, audit, and remediate our risk portfolio? Do we have standards in place to protect our assets throughout the ecosystem?

Thank you.

Christian Kjaer
cik@pwc.dk
+45 3945 3282

© 2013 PricewaterhouseCoopers LLP, a Delaware limited liability partnership. All rights reserved.

PwC refers to the United States 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.

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