# Stjórnun upplýsingaöryggis
# Innri og ytri kvaðir

7. febrúar 2014

Marinó G. Njálsson, CISA, CRISC

Hewlett-Packard Enterprise Security Services Nordic

# Það kemur ekkert fyrir mig!










# Um hvað snýst rekstur?

**Hér eru 3 lykilþættir:**

**Breytingastjórnun**

Að hafa stjórn á breytingum

**Áhættustjórnun**

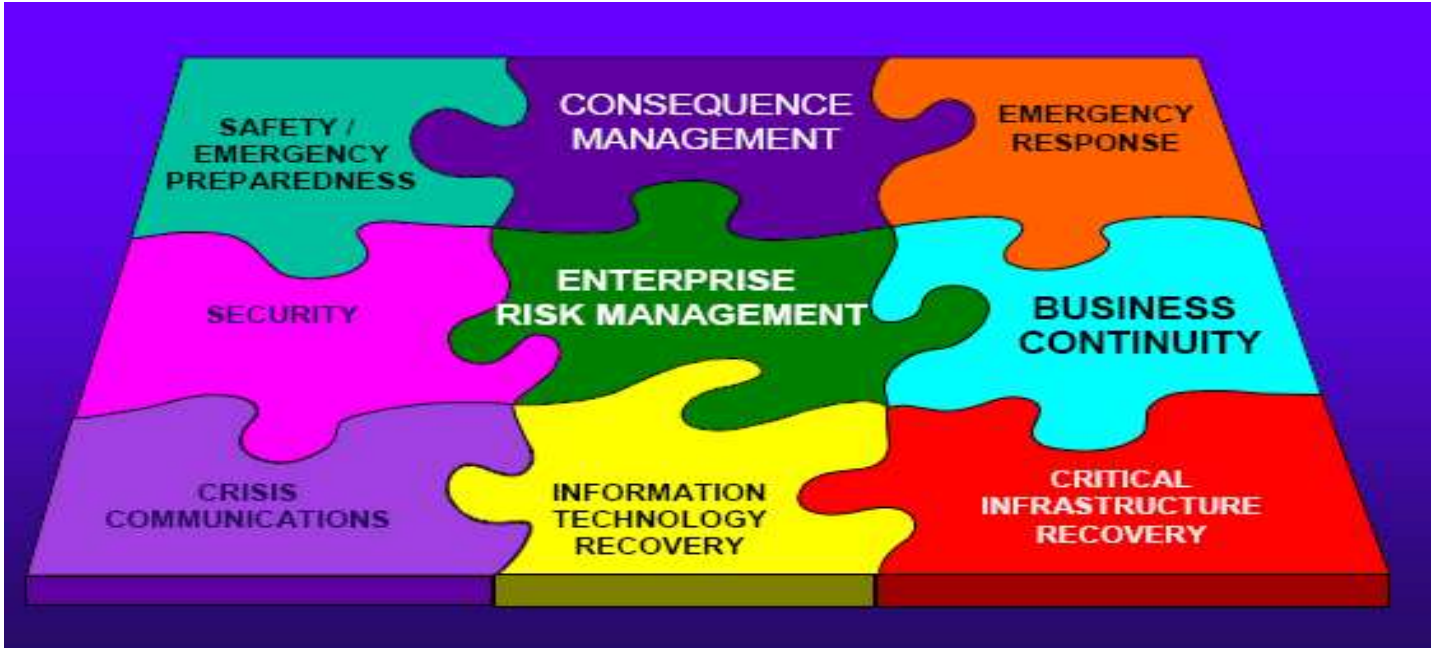
Að hafa stjórn á áhættu

**Stjórnun rekstrarsamfellu**

Að tryggja samfelldni rekstrar

**Öryggisstjórnun**
**Stjórnun upplýsingaöryggis**
**Stjórnun rekstraröryggis**

# Hvernig passar þetta inn í?



# Áhættustjórnun

## Skilgreining:

**Áhættustjórnun er samræmdar athafnir til að stýra og stjórna fyrirtæki með tilliti til áhættu**

**Áhættustjórnun felur að jafnaði í sér áhættumat, áhættumeðferð, áhættusamþykki og áhættusamskipti.**

ISO/IEC 27000:2012

# Stjórnun rekstrarsamfellu

**Skilgreining:**

**Stjórnun rekstrarsamfellu er heildstætt stjórnunarferli sem ber kennsl á möguleg áhrif sem ógna fyrirtæki og leggur til aðferðir til að byggja upp þol og getu til skilvirkra viðbragða sem verja hagsmuni hluthafa, lánadrottna, orðspor, vörumerki og verðmætasköpun.**

The Business Continuity Institute 2001

# Markmið áhættustjórnunar og stjórnunar rekstrarsamfellu

**Að tryggja áframhaldandi rekstur og lágmarka tjón, ef skaði verður.**

**Að uppfylla kröfur ytri aðila um trúnað, réttleika og tiltækileika upplýsinga**

**Hámarka arðsemi fjárfestinga og viðskiptatækifæra**

**Það er annars vegar gert með því að koma í veg fyrir eða lágmarka áhrif af atvikum sem geta truflað rekstur fyrirtækis og hins vegar með því að innleiða ráðstafanir í samræmi við ytri kröfur.**

# Innbyrðistengsl

- **Áhættustjórnun og stjórnun rekstrarsamfellu vinna saman**
- **Með áhættustjórnun er leitast við að stjórna áhættu í tengslum við lykilafurðir og -þjónustu fyrirtækisins**
- **Með því að einblína á áhrif truflana ber stjórnun rekstrarsamfellu kennsl á þær afurðir og þjónustu sem fyrirtækið treystir á varðandi afkomu og getur borið kennsl á hvað fyrirtækið þarf að gera til að standa við skuldbindingar sínar, m.a. með forvörnum**

# Hvers vegna að áhættustjórnun?

**Kannski er þetta ástæðan:**

**“Mín reynsla er…að fyrirtæki gera bara það sem þeim finnst algjörlega nauðsynlegt og vona að annað hrynji ekki”**

**Van Hauser of The Hacker’s Choice**
**Frá BBC World Service**

# Hvað viljum við verja?

**Þegar við erum að verja reksturinn gegn áföllum, þá erum við í raun að hlúa að:**

- **Orðspori**
- **Ímynd**
- **Markaðsvirði (þar sem það á við)**
- **Vörumerki**
- **Trúnaðargögn**
- **Viðskiptavild**
- **Fjárhag**
- **Framtíð rekstrarins**

# Uppruni öryggiskrafna

1. Viðskipta- og rekstrarlegar
2. Úr réttarreglum, s.s. lögum og reglugerðum, og samningum
3. Opinber fyrirmæli
4. Úr stöðlum og öðrum fyrirmælum
5. **Koma fram í áhættumati og áhrifagreiningu**

# Mikilvæg atriði

**Öryggisstjórnun verður að:**

- **vera eðlilegur hluti af stjórnun fyrirtækisins**
- **hæfa, einblína á og styðja við rekstrar- og viðskiptaleg markmið**
- **gera fyrirtækinu kleift að hámarka þjónustuframboð**
- **vera hagkvæm og virðisaukandi**
- **vera drifin áfram af eigendum rekstrarþátta og á ábyrgð þeirra**
- **endurspegla rekstrar- og viðskiptaleg áhrif af atvikum**

# Hvers vegna svona mikilvæg?

**Stjórnendur þurfa að spyrja sig:**

- **Hvað gerðir þú á morgun, ef allar upplýsingar fyrirtækisins glötuðust eða upplýsingakerfi yrðu óaðgengileg?**
- **Hver væri staða viðskiptavina þinna?**
- **Hver yrðu viðbrögð samkeppnisaðila?**
- **Hver yrðu viðbrögð banka, hluthafa, starfsfólks og annarra hlutaðeigandi?**

# Rannsóknir HP sýna að umfang ógna

**Stærð “svarta” markaðarins: $104ma[1]**

**Meðalsektir eru 270% af því sem eytt er í aðgerðir[2]**

**50% starfsmanna nota eigin búnað til að tengjast viðkvæmum viðskiptakerfum [3]**

1 Ponemon Institute: Mega Trends in Cyber Security Expert Opinion Study, May 2013
2 Ponemon Institute: Total Cost of Compliance Study, May 2012 (Organizations with more than 5,000 employees)
3 Ponemon Institute: Dangerous Insider Study, November 2012

# Viðfangsefni öryggisstjórnunar

**1** **Eðli og ástæða árása**
(hakkarar, leyniþjónustur)

**2** **Reglugerðaskógurinn**
(Aukin áhætta, kostnaður og flækja)

**3** **Breytt UT umhverfi**
(afhending og notkun breytist)

## Ný tegund andstæðinga


## Ytri kröfum eftirlitsaðila fjölgar

**PFS • Persónuvernd • Kauphöll**
**Basel III • PCI DSS/PA • ESB tilskipanir**

## Afhending

# Önnur viðfangsefni öryggisstjórnunar

| | |
|---|---|
| **Áhættustjórnun** | Strategic Risk Advisory, Account Security Officers, Client Security Officers, GRC Services, 3rd Party Compliance Management |
| **Atvikastjórnun** | Digital Investigation, Forensics, SEIM, SIEM Management Breach and Incident Response |
| **Ógna- og veikleika-stjórnun** | Private SOC Consultancy, Vulnerability Scanning and Intelligence, Monitoring, DDoS |
| **Persónuvernd** | Data Loss Protection, Web and email Management, Endpoint Threat Management (Encryption, AV) |
| **Auðkenning og aðgangur** | Identity Access Management, User Access Management, 2-Factor Management, Identity Governance |
| **Öryggi hugbúnaðar** | Web Application Monitoring, Web Application Scanning, Application Testing, Secure Applications Development |
| **Öryggi innviða og neta** | Infrastructure Security, Perimeter Management, Remote Access Management, Cloud Security Assessment, Secure Mobility |

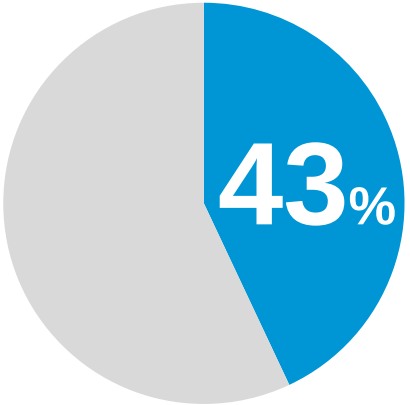
# Hvers vegna gengur illa að bregðast við?

Margbreytileg tækni

Skortur á hæfu starfsfólki

Breytt umhverfi

Erfitt að sjá þróun fyrir



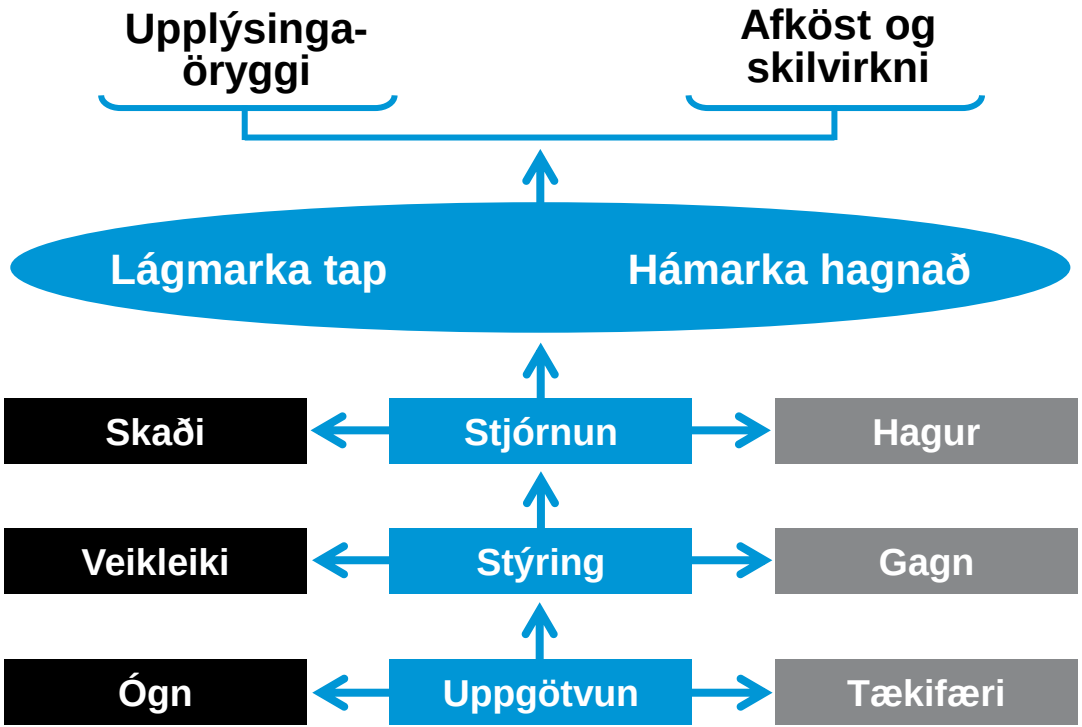

**Upplýsingaáhætta dregur úr sveigjanleika fyrirtækja:**
Sammála: 43%

[3]Source: Economist Intelligence Unit, 2013

# Öryggisstjórnun á erindi við stjórn

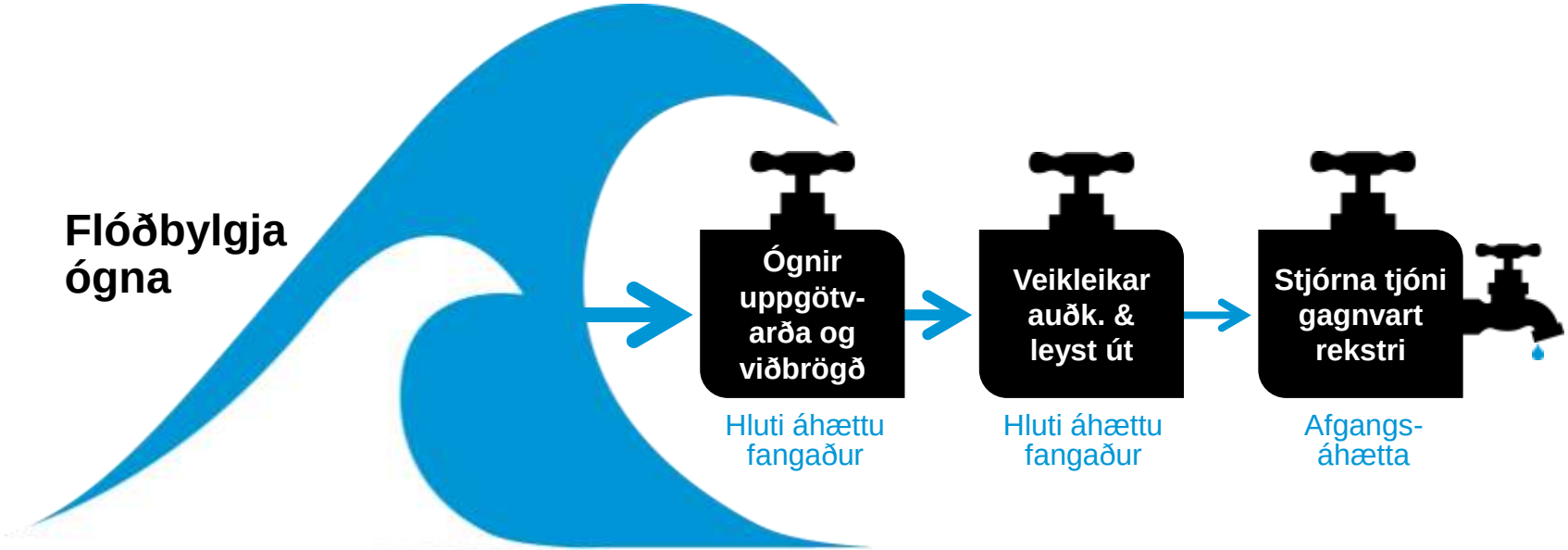
# Markmið öryggisstjórnunar

Lágmark neikvæð áhrif og hámarka jákvæð áhrif

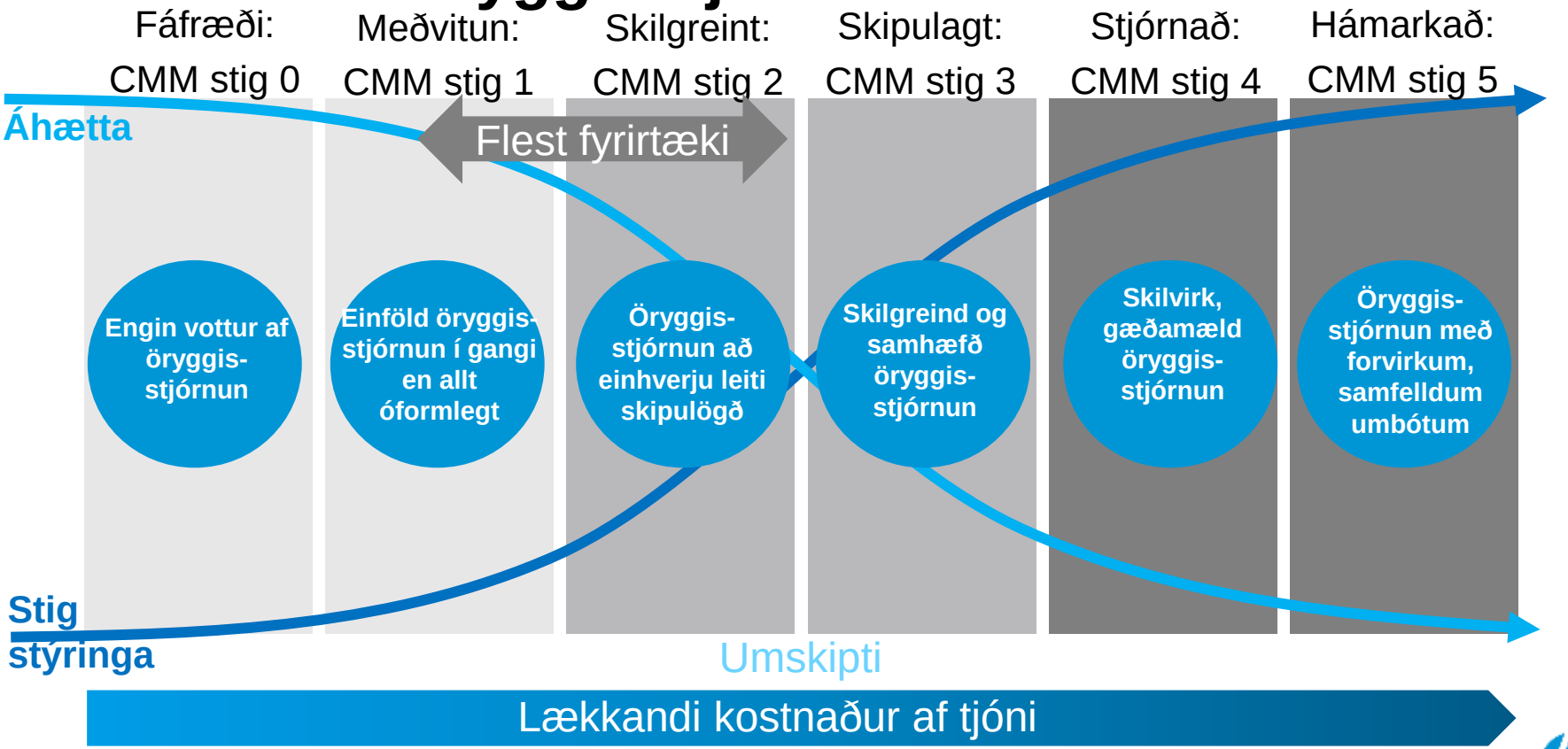


# Með því að stjórna áhættu

**Upplýsingaáhætta = ógn x veikleiki x líkur á tjóni**



# Þroskalíkan öryggisstjórnunar



# Ávinningur af öryggisstjórnun

- Færri óvæntar uppákomur
- Dregur úr áhrifum og líkum á atvikum
- Nýta tækifærin
- Bætt skipulagning, frammistaða og árangur
- Hagkvæmni og skilvirkni
- Bætt samskipti við hagsmunaaðila
- Bætt orðspor
- Ábyrgni, fullvissa og stjórnun
- Sönnun fyrir faglegum stjórnháttum
- Bætir verkferla
- Bætir þjónustu við viðskiptavini
- Skapar forskot í samkeppni
- Losar um tíma stjórnenda sem áður fór í að slökkva elda
- Eykur tiltrú á framtíðina
- Getur lækkað fjármagnskostnað

**Og þetta er áður en atvik á sér stað!**

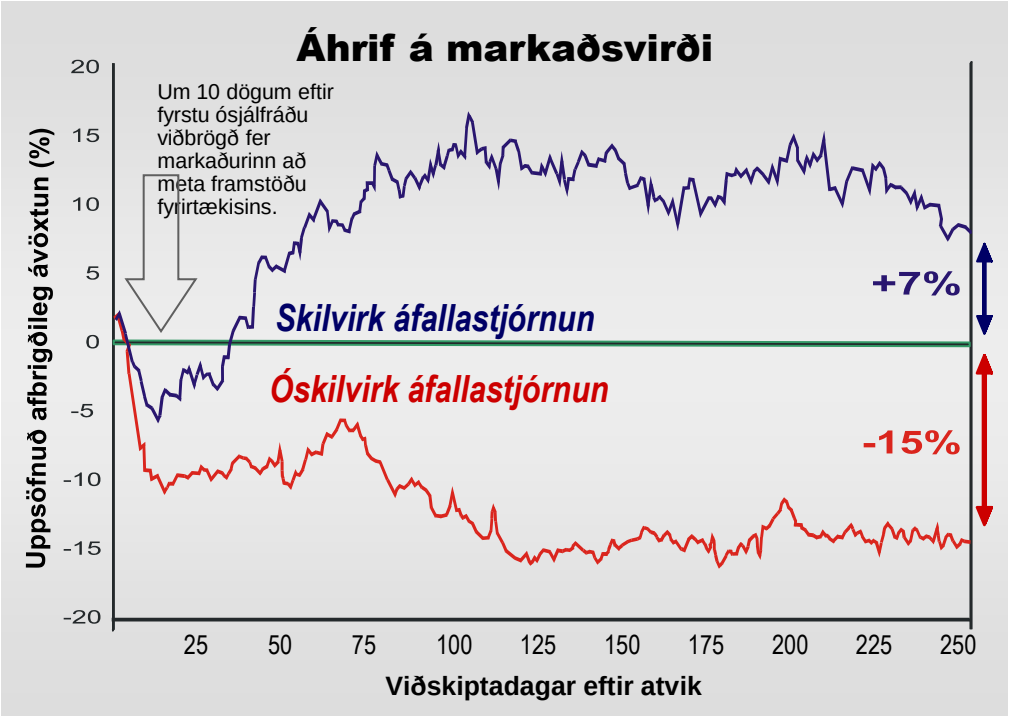
**Eftir atvik er hægt að meta haginn í milljónum!**

# Ávinningur af öryggisstjórnun

**Mestar líkur eru á að allir stjórnendur eigi eftir að standa frammi fyrir áfalli.**

**Geta til að hafa stjórn í áfalli ber vott um góða stjórnhætti fyrirtækis vegna:**

- **Mikilla skjótra áhrifa á markaðsvirði**
- **Langtíma áhrif á orðspor**




Heimild: 'The Impact of Catastrophes on Shareholder Value', Rory F. Knight & Deborah J. Pretty, Templeton College, University of Oxford

# Stjórnun upplýsingatækni/-öryggis

**IT Governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structure and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.**

**IT Governance Implementation Guide**
**IT Governance Institute**

# Góð leið til að viðhalda samkeppnishæfni

Þróun hlutabréfaverðs þeirra 20% fyrirtækja í norrænum kauphöllum sem standa sig best og verst í að innleiða góða stjórnunarhætti

# Spurningar?



# Takk fyrir