



**Security
Practitioners**

Protect information assets,
brand, revenue and reputation

The Changing Role of the CISO

Cyber Maryland Conference 2013
Baltimore MD

Dr Claudia Natanson
Security Practitioners Ltd

5 reasons to explore this topic



1

Current market demand for the CISO role.



2

Notable change in CISO role over the last decade.



3

Means of benchmarking your own CISO role.




4

Exploring ways to improve CISO effectiveness at senior levels.



5

Exploring ways to improve range of CISO influence across the organisation.



Let's look
at some
of the facts

Using the Results of some industry surveys



- PWC 2014 “The Global State of Information Security Survey 2014”.



- 2013 US State of Cybercrime Survey



- IBM Center for Applied Insights

Today we are looking at some of the output from these surveys, to highlight and benchmark our own practices.

It will give us a chance to discuss whether we agree with the results, and if we do, to look at the impact on these and other challenges on the CISO role.



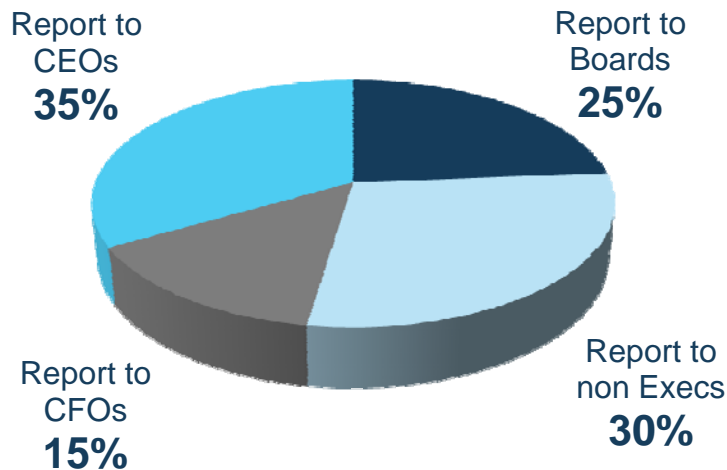
The Reporting line of the CISO has changed

Boards understand risk...they get it but.....

The question for the CISO is whether from your position in the organisation are you able to directly contribute to business risk discussions?

If you are, this is good as it **increases your knowledge** of the organisation's risk appetite. It also means more access to and greater respect from your C-level peers?

SUMMARISED STATISTICS



From Wikipedia and PWC report on security best practices 2011

HIGH LEVEL OF INFLEUNCE



LOWER LEVELS OF INFLEUNCE

Reporting Lines: The debate

CIO

Driver: Security still seen as technology

Implementation of roles often experience a conflict of interest.

CEO

Driver: Security is a key risk & board agenda item

Possible expectation that a utopian state of security is achievable

Reporting Lines: Goals



Managing Expectations at C-Level

The PWC 2014 report shows that..

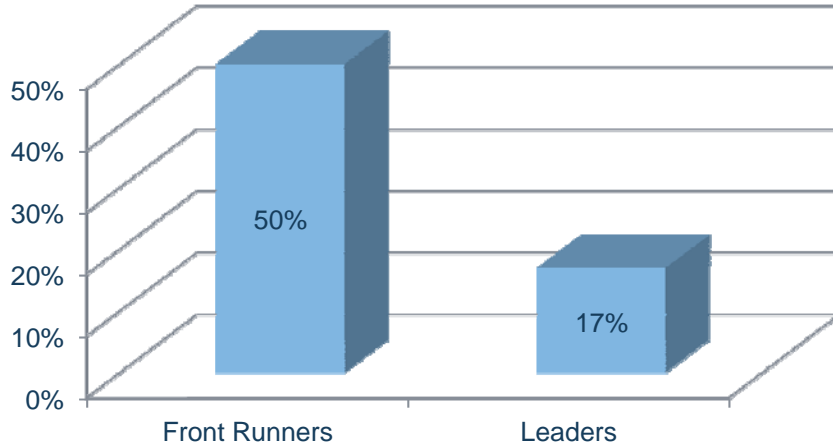
1

74% respondents believe their security effective-top execs even more optimistic

2

Half the respondents consider themselves “front runners” ahead of the pack in strategy & security practices

Adapted from PWC 2014 Report



Leaders Defined as having:-

- An overall security strategy
- A CISO or equivalent reporting to a CEO< CFO, COO, CRO or legal counsel.
- Measured and reviewed the effectiveness of security within the past year.
- An understanding of exactly what type of security events have occurred in the past year.

The analysis showed that there were significantly fewer real leaders than self-identified front runners.

Check list: Do we have a clear plan and strategy?

5 areas for deciding the CISO strategy



- Dependent on reporting line
- Culture of the organisation
- Resources-people & funding
- Exec Support and Sponsorship
- Professional and Personal Confidence of the CISO

Finding a strategic voice

Security leaders see significant change ahead

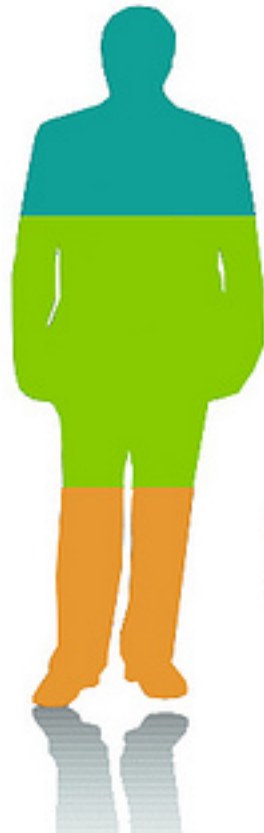
Nearly two-thirds say **senior executives** are paying **more attention** to security issues.

2/3s expect to **spend more** on security over the next two years.

External threats are rated as a **bigger challenge** than internal threats, new technology or compliance.

More than one-half say **mobile security** is their greatest near-term **technology concern**.

And their roles are evolving with growing authority, accountability and impact across the enterprise.



Influencers

Confident and prepared, influence the business strategically

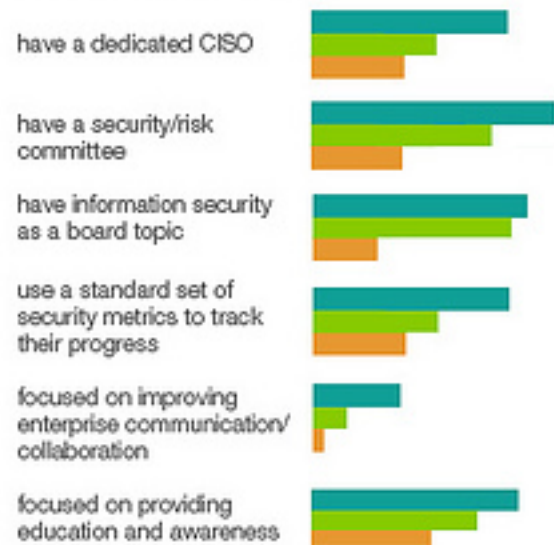
Protectors

Less confident, prioritize security strategically but lack necessary structural elements

Responders

Least confident, focus largely on protection and compliance

How they differ



Tick in the box or embedded and visible security?



- Policy implementation is political, and should be implemented only after time spent discussing and soliciting buy-in.
- Quoting ISO/IEC compliance without visible demonstration starting at the top is useless. Time must be spent winning heart and minds top down. Great investment.
- If you have to provide too many policy exceptions, it means the policy isn't realistic.
- With new technologies and initiatives, controlled exceptions driven by exec ownership provides caveats at CISO level.
- Having no policies is unforgivable.

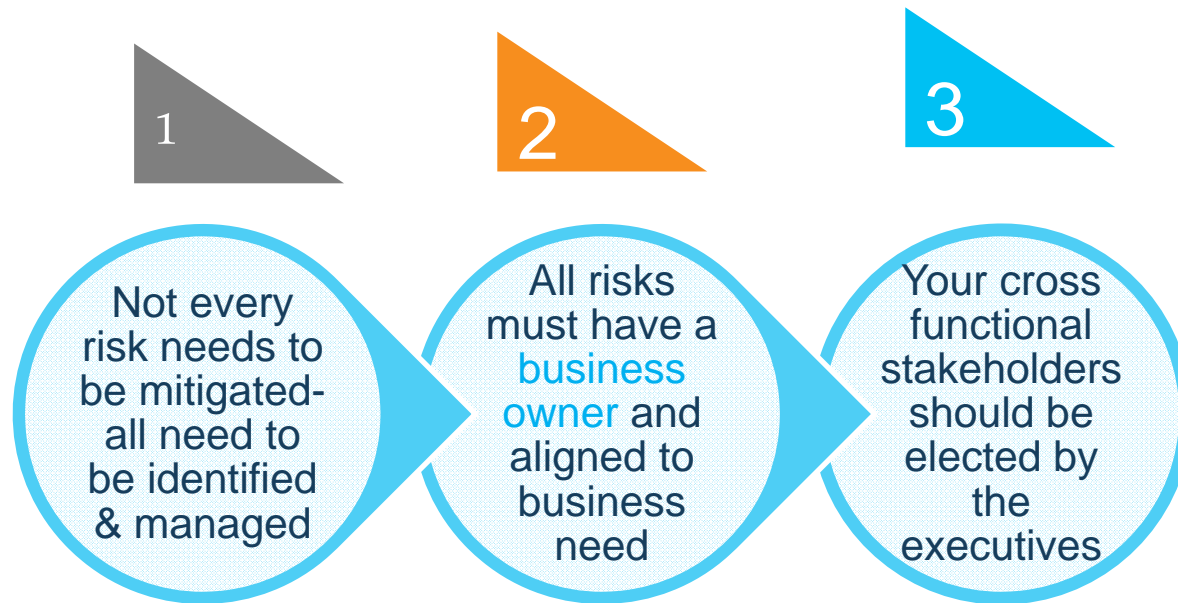
A US-only survey shows that, even when in place, security technologies and policies often do not prevent incidents.


Respondents to the 2013 US State of Cybercrime Survey¹, co-sponsored by PwC, say security incidents increased 33%, despite implementation of security practices. For many, existing security technologies and policies are simply not keeping pace with fast-evolving threats

Security technologies and policies in place (US only)

Use policy-based network connections to detect and/or counter security incidents	68%
Inspect inbound and outbound network traffic	61%
Use account/password management in an attempt to reduce security incidents	60%
Have an acceptable-use policy	55%
Use malware analysis as a tool to counter advanced persistent threats (APTs)	51%
Use data loss prevention technology to prevent and/or counter security incidents	50%
Use cyber-threat research in an attempt to reduce security incidents	25%
Do not allow non-corporate-supplied devices in the workplace/network access	17%

Aligning Security with Business Need





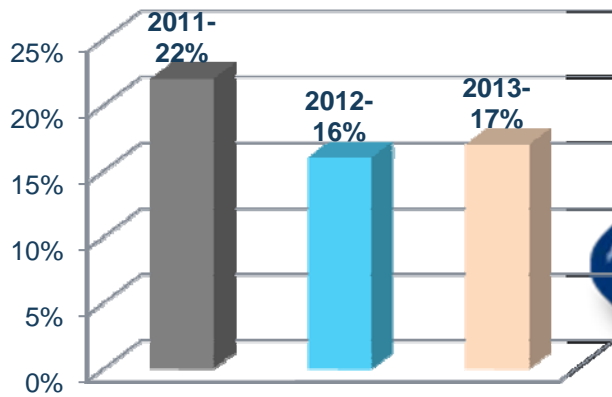
Staying one
step ahead

Have Strategies for these areas now...

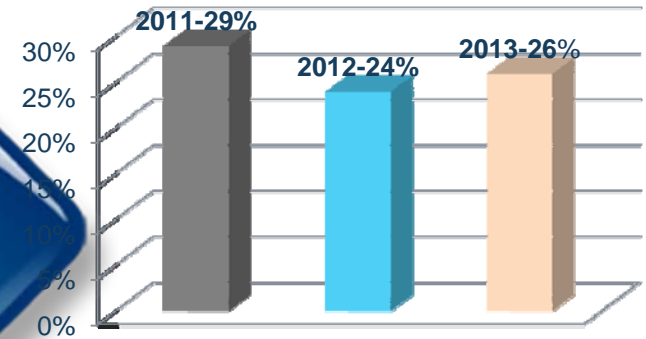
Information Classification and Handling

The PWC 2014 report shows that many respondents are not adequately safeguarding their high-value information.-have not implemented basic policies to protect intellectual property

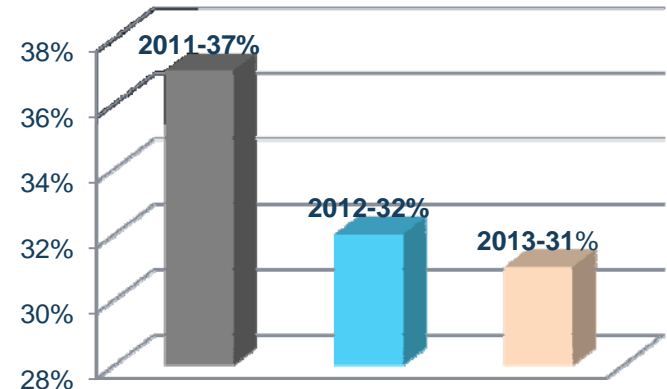
Classifying business value of data



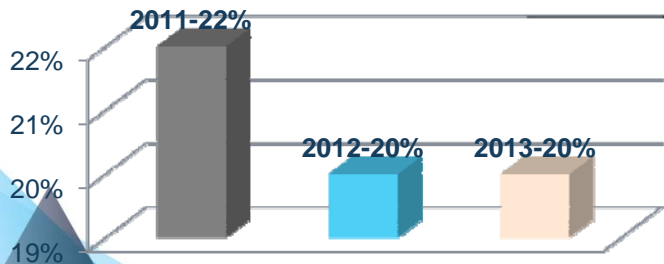
Inventory of assets/asset management



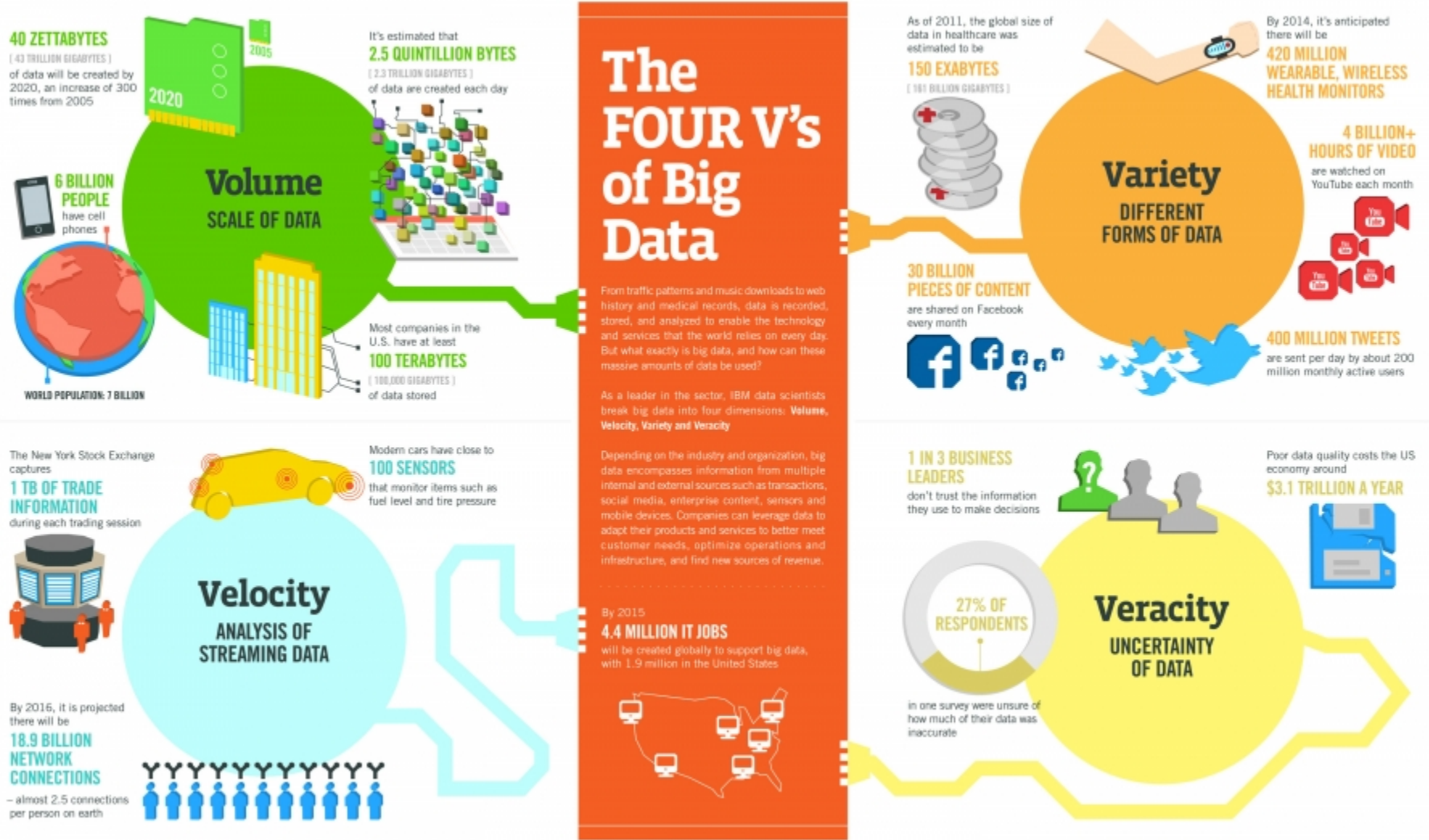
Regular review of users and access



Procedures dedicated to protecting IP



The BIG DATA CHALLENGE- IBM's View



Sources: McKinsey Global Institute, Twitter, Cisco, Gartner, EMC, SAS, IBM, MCPTEC, GIG



Cost Efficiencies or Security challenges?

Savings on upfront costs for mobile implementation

Sales improve with use of iPads

Has helped to improve business competitive edge

BYOD

Bring your own device



Concern about loss of Confidential data

Employee or employer liability

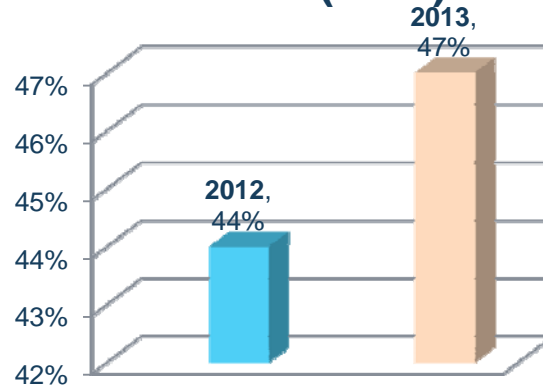
Maintenance costs debate

Cloud Computing is here to stay

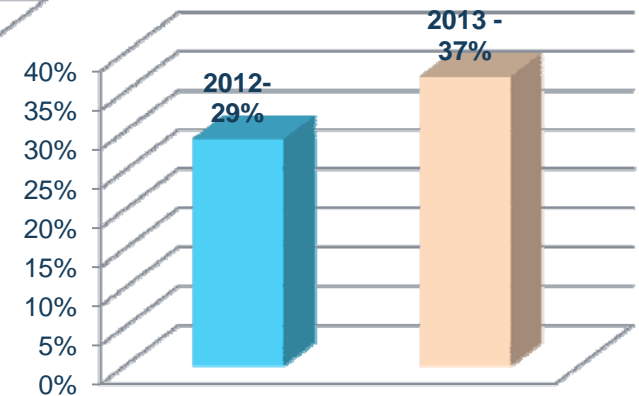
PWC report states that half of the respondents use cloud computing but they often do not include in their security policies



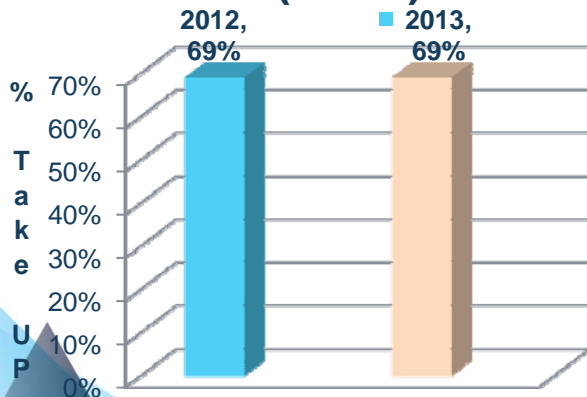
Infrastructure-as-a-Service (IaaS)



Platform-as-a-Service (PaaS)



Software-as-a-Service (SaaS)



Summary



Key References

- *IBM Data from IBM Center for Applied Insights Study*
“Finding a strategic voice” Insights from the 2012 IBM CISO Assessment
- *Key findings from The Global State of Information Security® Survey 2014*
September 2013
- *2013 US State of Cybercrime Survey*, co-sponsored by CSO magazine, CERT Coordination Center at Carnegie Mellon University, Federal Bureau of Investigation, PwC, and the US Secret Service, March-April 2013

Thank You

Q & A

