Cyber Assurance - what should the IT auditor focus on?

Berthing, Hans Henrik

Publication date:
2014

Document Version
Early version, also known as pre-print

ISACA®
Trust in, and value from, information systems

protiviti®
Risk & Business Consulting.
Internal Audit.

CYBER ASSURANCE - WHAT SHOULD THE IT AUDITOR FOCUS ON?

Hans Henrik Berthing, CPA, CISA, CGEIT, CRISC, CIA| 12.Nov.2014

WELCOME!

Have a question? Use the Ask A Question button

Audio is streamed over your computer

Technical Issues? Click the ? Button

Use the Feedback button to share your comments about today's event!

Questions or Suggestions?
Email them to eLearning@isaca.org

Use the Attachments Button to find the following:

- PDF Copy of Today's Presentation
- Link to the Event Home Page where ISACA members can find the CPE Quiz
- Complete the Webinar Survey
- MORE Assets from today's speaker
- Upcoming ISACA Events

TOP PRIORITIES FOR TODAY'S INTERNAL AUDIT FUNCTIONS

Social media, mobile applications, cloud computing and security are critical areas of concern

KEY RISKS POSED BY SOCIAL MEDIA USE	Level of severity (10-pt. scale)
✔ Financial loss	7.3
✔ Business continuity	6.9
✔ Intellectual property loss	6.6
✔ Employee productivity	6.1
KEY AREAS FOR IMPROVEMENT	**Competency Level (5-pt. scale)**
✔ Mobile apps	2.6
✔ NIST Cybersecurity Framework	2.4
✔ Social media applications	2.8
✔ Cloud computing	2.8

Social media applications and related risks are top priorities for internal auditors to address, as are risks surrounding mobile applications, cloud computing and security

As indicated in past years of our study, internal auditors plan to strengthen their knowledge of computer-assisted auditing tools, and continuous auditing and monitoring techniques

CAATs and data analysis remain on center stage

KEY AREAS FOR IMPROVEMENT	Competency Level (5-pt. scale)
✔ Computer-assisted audit tools	3.0
✔ Data analysis tools – data manipulation	3.1
✔ Data analysis tools – statistical analysis	3.1
✔ Auditing IT – new technologies	3.2
✔ Data analysis tools – sampling	3.2

Fraud management efforts focus on technology

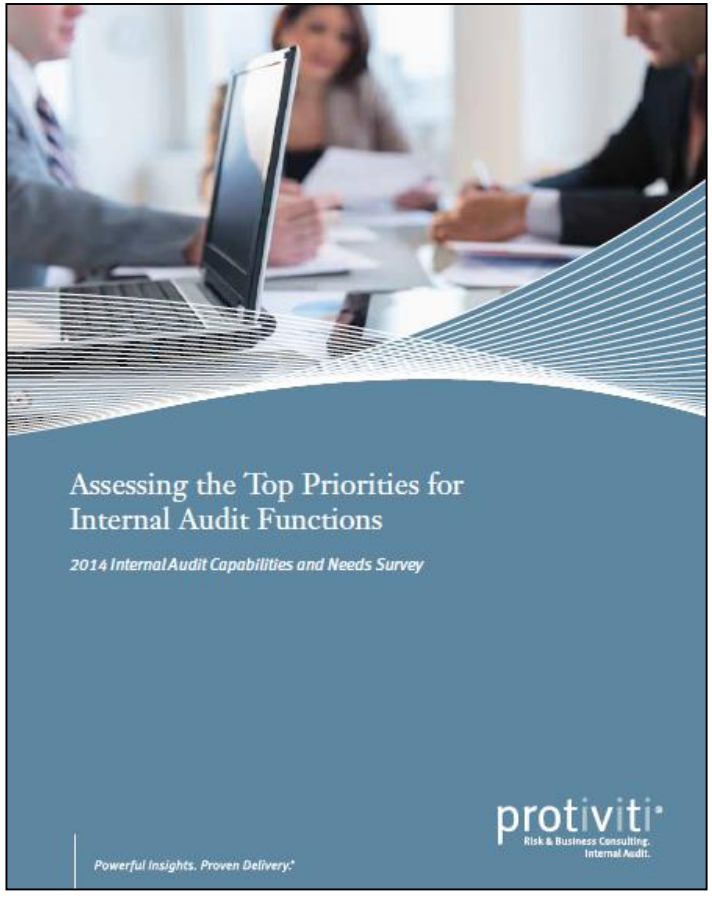
KEY AREAS FOR IMPROVEMENT	Competency Level (5-pt. scale)
✔ Continuous auditing	3.2
✔ Continuous monitoring	3.2
✔ Fraud monitoring	3.3
✔ Fraud auditing	3.4
✔ Fraud detection/investigation	3.3

Auditors are concentrating more time and attention on fraud prevention and detection in increasingly automated business environments and workplaces

Source: *"2014 Internal Audit Capabilities and Needs Survey" (March 2014)*

ISACA®
Trust in, and value from, information systems

2014 INTERNAL AUDIT CAPABILITIES AND NEEDS SURVEY



For more information on this publication, please visit www.protiviti.com/IAsurvey

ISACA
Trust in, and value from, information systems

HANS HENRIK BERTHING

- Married with Louise and dad for Dagmar and Johannes
- CPA, CRISC, CGEIT, CISA and CIA
- ISO 9000 Lead Auditor
- Partner and owner for Verifica
- Financial Audit, since 1994 and IT Assurance since 1996
- Member of FSR IT Advisory Board
- ISACA IT Assurance Task Force
- Instructor, facilitator and speaker
- Senior Advisor & Associated professor Aalborg University (Auditing, Risk & Compliance)

ISACA®
Trust in, and value from, information systems

AGENDA SLIDE

1. Cybercrime
2. Cyber Governance
3. IT Assurance
4. Cyber Crime assurance
5. Cloud Governance

BUSINESS BENEFITS OF CLOUD COMPUTING

- **Cloud strategies make the enterprise more efficient and agile.**
- **Cloud computing allows delivered services to be more innovative and more competitive.**
- **Cloud computing reduces overall operating costs.**
- **How confident can boards be that management plans will achieve these benefits?**

Source: CLOUD GOVERNANCE: Questions Boards of Directors Need to Ask, 2013, ISACA

GOVERNANCE AND CHANGE ISSUES WITH CLOUD COMPUTING

- Strategic direction of the business and of IT
- Changes to meet performance objectives
- IT is aligned with the business
- Systems are secure
- Risk is managed

Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

BOARD AND CYBERSECURITY

“A primary responsibility of every board of directors is to secure the future of the organization. The very survival of the organization depends on the ability of the board and management not only to cope with future events but to anticipate the impact those events will have on both the company and the industry as a whole.”

Tom Horton

CYBERCRIME

•Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. – Interpol

- Attacks against computer hardware and software, for example, botnets, malware and network intrusion;
- Financial crimes, such as online fraud, penetration of online financial services and phishing;
- Abuse, especially of young people, in the form of grooming or 'sexploitation'.

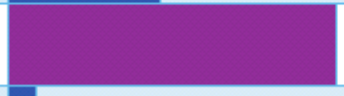
•Cybercrime reports continue to rise. Fourth-most reported type of crime in PWC's 2014 Crime survey. Cybercrime is not just a technology problem. It is a business strategy problem.

•Oil and energy industry in Norway is under attack, August 30, 2014

•Cyber Security for Nuclear Power Plants, US, January 2012

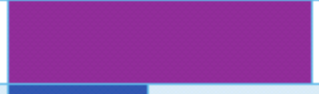
•Convention on Cybercrime, As of October 2014, 44 states have ratified the convention, while a further nine states had signed the convention but not ratified it

THE BOARD'S PERCEPTION OF CYBERSECURITY RISKS OVER THE LAST ONE TO TWO YEARS

Response	Chart	Frequency	Count
Has been at a high level		8.5%	160
Increased significantly		18.7%	353
Increased		**40.8%**	**772**
Decreased		2.0%	38
Decreased significantly		1.1%	20
No change		28.9%	547
Not Answered			45
		Valid Responses	**1,890**
		Total Responses	**1,935**

Source: IIA's Audit Executive Center "Pulse of the Profession 2014"

BOARD INVOLVEMENT DURING THE LAST FISCAL YEAR IN REGARD TO SPECIFIC ACTION OR REQUEST ON CYBERSECURITY PREPAREDNESS?

Response	Chart	Frequency	Count
Actively involved		14.1%	267
Involved		34.9%	662
Minimally involved		**36.1%**	**686**
Not sure of involvement		14.9%	283
Not Answered			37
		Valid Responses	**1,898**
		Total Responses	**1,935**

58% of the respondents said that they should be actively involved in cybersecurity matters.

Source: IIA's Audit Executive Center "Pulse of the Profession 2014"

FIVE PRINCIPLES FOR CORPORATE BOARDS: "AS THEY SEEK TO ENHANCE THEIR OVERSIGHT OF CYBER RISKS"

1. **Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.**

2. **Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.**

3. **Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.**

4. **Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget.**

5. **Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.**

The National Association of Corporate Directors (NACD), in conjunction with the American International Group (AIG) and the Internet Security Alliance (ISA), 2014

SIX QUESTIONS THE BOARD SHOULD ASK

1. Does the organization use a security framework?
2. What are the top five risks the organization has related to cybersecurity?
3. How are employees made aware of their role related to cybersecurity?
4. Are external and internal threats considered when planning cybersecurity program activities?
5. How is security governance managed within the organization?
6. In the event of a serious breach, has management developed a robust response protocol?

Cybersecurity what the Board of Directors need to ask, IIARF Research Report, 2014

POTENTIAL RISK AREAS

1. Proliferation of BYOD and smart devices
2. Cloud computing
3. Outsourcing of critical business processes to a third party (and lack of controls around third-party services)
4. Disaster recovery and business continuity
5. Periodic access reviews
6. Log reviews

Cybersecurity what the Board of Directors need to ask, IIARF Research Report, 2014

COMMON CYBERCRIMINAL ATTACK VECTORS

- Application vulnerabilities
- Remote access.
- Ineffective patch management
- Weak network security/flat networks
- Lack of real-time security monitoring
- Third parties
- Lack of a data retention policy

INFORMATION ASSURANCE AND CYBERSECURITY

- **Protecting the most important digital information assets**
- **According to the Department of Homeland Security, cyber intrusions and attacks have increased dramatically over the last decade, exposing sensitive personal and business information, disrupting critical operations, and imposing high costs on the economy. Anyone connected to the internet is vulnerable.**
- **Various research is identifying new ways to protect critical public and private information infrastructure; helping organizations monitor potential security risks; and developing courses and real-world simulations to educate information assurance and Cybersecurity professionals**

EXPERTISE AND RESEARCH IN INFORMATION ASSURANCE AND CYBER SECURITY

- Risk assessment and management
- Developing security policies and rights management systems
- Identifying security awareness issues within organizations and recommending processes to overcome them
- Implementing or integrating security tools and applications
- Assessing software and information architecture for security
- Assessing network security
- Implementing intrusion detection, forensics and timely response processes
- Protecting privacy and increasing awareness
- Implementing next generation infrastructure and applications
- Detection of emerging opinions and opinion leaders in emerging media

IT ASSURANCE TASKS

- IT Governance and Assurance
- IT Security Strategy and policies/guidelines
- Implementation
- Project risk management
- Cyber Assurance
- Assessment of maturity and GAP analysis
- Risk workshop
- Facilitator

UNDERSTAND THE BUSINESS & INTERNAL CONTROLS – ISA 315

- In understanding the entity's control activities, the auditor shall obtain an understanding of how the entity has responded to risks arising from IT. - 21

- Use of IT (a potential related business risk might be, for example, that systems and processes are incompatible). – A39

- Management's failure to commit sufficient resources to address IT security risks may adversely affect internal control by allowing improper changes to be made to computer programs or to data, or unauthorized transactions to be processed – A82

- The use of IT affects the way that control activities are implemented. From the auditor's perspective, controls over IT systems are effective when they maintain the integrity of information and the security of the data such systems process, and include effective general IT-controls and application controls. – A103

- Inconsistencies between the entity's IT strategy and its business strategies. – APP 2

IT BENEFITS AN ENTITY'S INTERNAL CONTROL

- Consistently apply predefined business rules and perform complex calculations in processing large volumes of transactions or data;
- Enhance the timeliness, availability, and accuracy of information;
- Facilitate the additional analysis of information;
- Enhance the ability to monitor the performance of the entity's activities and its policies and procedures;
- Reduce the risk that controls will be circumvented; and
- Enhance the ability to achieve effective segregation of duties by implementing security controls in applications, databases, and operating systems.

Source: ISA 315 – A62

IT POSES SPECIFIC RISKS TO INTERNAL CONTROL

- Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.

- Unauthorized access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized or non-existent transactions, or inaccurate recording of transactions. Particular risks may arise where multiple users access a common database.

- The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties.

- Unauthorized changes to data in master files or to systems or programs.

- Failure to make necessary changes to systems or programs.

- Inappropriate manual intervention.

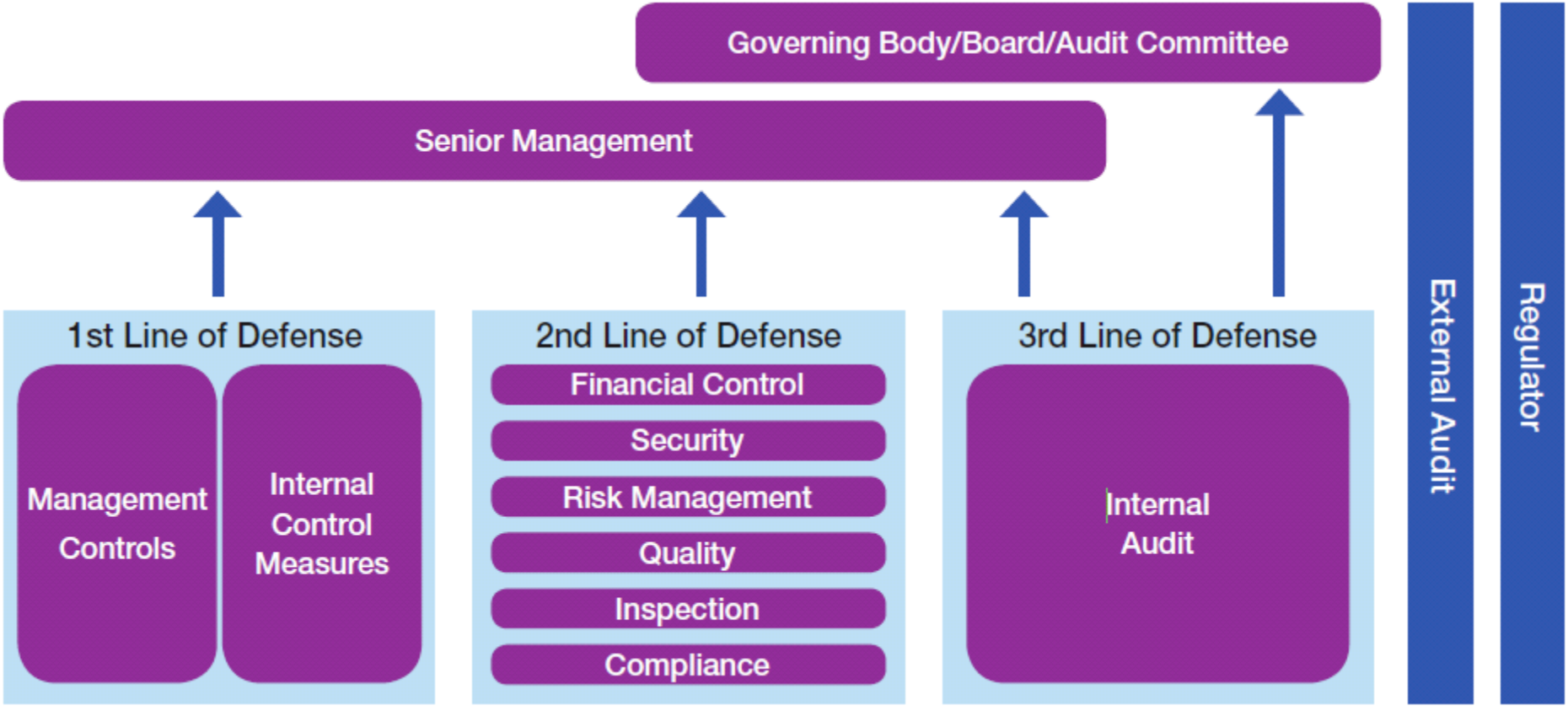
- Potential loss of data or inability to access data as required.

Source: ISA 315 – A63

IT ENVIRONMENT

- **People and organization**
- **Applications and infrastructure**
- **IT processes**
- **Understanding of the IT environment and its planned changes (IT strategies)**
- **Work relating to the IT environment depends of likelihood of material business and audit risks and complexity of the IT environment**
- **Document the work**
  - Complexity of IT environment (in addition to local guidance)
  - Changes in the IT environment (IT strategy/action plans)
  - Organization of the IT function
  - Regulatory requirements

IIA THIRD LINE OF DEFENSE



CYBERCRIME AUDIT/ASSURANCE PROGRAM

1. Planning and Scoping the Audit
2. Understanding Supporting Infrastructure
3. Governance
4. Organization
5. Organizational Policies
6. Business Role in Cybercrime Prevention
7. IT Management
8. Incident Management Policy And Procedures
9. Incident Management Implementation
10. Crisis Management

GOVERNANCE QUESTIONS ABOUT CLOUD

1. Do management teams have a plan for cloud computing? Have they weighed value and opportunity costs?

2. How do current cloud plans support the enterprise's mission?

3. Have executive teams systematically evaluated organizational readiness?

4. Have management teams considered what existing investments might be lost in their cloud planning?

5. Do management teams have strategies to measure and track the value of cloud return vs. risk?

Source: CLOUD GOVERNANCE: Questions Boards of Directors Need to Ask, 2013, ISACA

TRUE ABOUT PRIVATE CLOUD, PUBLIC CLOUD AND HYBRID CLOUD (N =904)

	The benefit outweighs the risk.	The risk outweighs the benefit.	The risk and benefit are appropriately balanced.
Public cloud	12%	**68%**	20%
Hybrid cloud	16%	40%	**44%**
Private cloud	**57%**	10%	33%

Source: IT Risk/Reward Barometer: Europe, 2012, ISACA (n=980)

BUSINESS CHALLENGES TO CONSIDER

Challenge	Description
Incompatibility	Cloud services may not be compatible with the existing IT infrastructure or specific systems that must be integrated.
Uptime	Cloud vendors may not be able to guarantee agreed-on uptime. In addition, uptime may be impacted by other factors, including the customer's Internet service providers.
Performance	Multitenant models can degrade performance over time if capacity is not properly planned. Internet speed can also negatively impact performance.
Security	Cloud computing represents traditional and new risk that must be accounted for and mitigated accordingly (either by the CSP or the customer).
Compliance	The ubiquitous and abstract nature of the cloud can cause an enterprise's transition from compliance to noncompliance without any notice.
Pay-as-you-go	The enterprise must implement controls to avoid overage charges incurred when systems stay connected after a demand spike is over.
Lock-in (hardware or vendor)	Customers may become locked into a specific technology or a specific cloud vendor, which can prevent portability.
Cloud consumerization	Business units may be able to procure cloud services without involving IT. To prevent this situation, the enterprise must adapt its governance framework to control cloud services procurement.
Limited customization (Black Box)	Cloud applications may not be customized every time the business process changes, making the business process a "Black Box" due to costs associated with each modification or application limitations.

Source: ISACA Cloud Computing Vision Series White Paper July 2012

RISKS AND SECURITY CONCERNS WITH CLOUD COMPUTING

- Reputation, history and sustainability of the provider
- Failure to perform to agreed-upon service levels
- Where information actually resides
- Third-party access to sensitive information
- Compliance to regulations and laws in different geographic regions (Public Clouds)
- Information may not be immediately located

Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

ASSURANCE CONSIDERATIONS

- Transparency
- Privacy
- Compliance
- Trans-border information flow
- Certification

Source: Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives, 2009, ISACA

POSITIVE AND NEGATIVE INFLUENCES ON CLOUD ADOPTION AND INNOVATION

Positive Influence on Cloud Adoption/Innovation		Mean Score	Rank	Negative Influence on Cloud Adoption/Innovation	Mean Score	Rank
Cost management	Proces	3.77	1	Information security	4.22	1
Agility	Bus Growth	3.75	2	Data ownership/custodian responsibilities	4.12	2
Time to market	Bus Growth	3.73	3	Legal and contractual issues	4.04	3
Efficiency	Proces	3.65	4	Regulatory compliance	4.01	4
Productivity	Proces	3.61	5	Information assurance	3.77	5
Business unit demand	Bus Growth Proces	3.55	6	Longevity of suppliers	3.44	6
Resilience	Bus Growth	3.52	7	Contract lock-in	3.42	7
New technology	Bus Growth	3.46	8	Performance standards	3.30	8
Customer demand	Proces	3.42	9	Disaster recovery/business continuity	3.25	9
Technical resources	Bus Growth	3.37	10	Performance monitoring	3.21	10
New markets		3.33	11	Technology stability	3.10	11
	Summary Mean	**3.56**			**Summary Mean**	**3.62**

Source: Cloud Computing Market Maturity *Study Results, 2012, ISACA & CSA*

PERSPECTIVES ON SECURITY AND ASSURANCE COMPONENTS

Security and Assurance Component	Overall Rank	User Rank	Provider Rank
Concerns for multitenancy	10	12	11
Information security	12	7	17
Testing and assurance	18	18	18
Data ownership/custodian responsibilities	22	22	23
International data privacy	25	25	26

Security and Assurance Component	Overall Rank	Business Rank	Security Rank	Technology Rank
Concerns for multitenancy	10	13	15	8
Information security	12	11	14	13
Testing and assurance	18	22	10	21
Data ownership/custodian responsibilities	22	23	23	19
International data privacy	25	25	27	25

ADDITIONAL RESSOURCES

- Cybersecurity Nexus, ISACA
- Cybercrime Audit Assurance Program, 2012, ISACA
- Cybersecurity What the Board of Directors Needs to Ask, 2014, IIARF Research Report
- Transforming cybersecurity using cobit5, 2013, ISACA
- US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey, PWC
- PwC's 2014 Global Economic Crime Survey
- Interpol and National Cyber Crime Investigation & Research
- Responding to Targeted Cyberattacks, 2014, ISACA & EY
- Plus many more

SUMMARY

- Cyber Governance & Assurance business critical
- Where and how to add value and manage risk for the business.
- Organization of any scale can be cyber attacked
- Ask Cyber & cloud-specific questions to B-o-D ans C-suite
- Cloud computing are aligned to the enterprise strategy.
- Security and assurance.
- Keep updated via research and white paper

THANK YOU FOR ATTENDING THIS WEBINAR

protiviti®
Risk & Business Consulting.
Internal Audit.

FOR **MORE** GO TO:
www.isaca.org/webinars

LEARN MORE

Hans Henrik Aabenhus Berthing
Statsautoriseret revisor | CGEIT | CRISC | CISA | CIA
Phone +45 35 36 33 56 | Cell +45 22 20 28 21 |
E-mail hhberthing@verifica.dk

Verifica Statsautoriseret Revisionsvirksomhed

ISACA®
Trust in, and value from, information systems