Cyber Assurance - what should the IT auditor focus on?

Hans Henrik Berthing, CPA, CISA, CGEIT, CRISC, CIA
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
- Associated professor Aalborg University (Auditing, Risk & Compliance)
AGENDA SLIDE

- Cybercrime
- Cyber Governance
- IT Assurance
- Cyber Crime assurance
- Cloud Governance
LEARNING OBJECTIVES

• Know what cyber- and cloud-specific questions the BoD and C-suite need to ask
• Understand the potential areas of risk that an organization has related to cybersecurity
• Learn how the IT Auditor can provide assurance over cybersecurity issues
• Learn the assurance considerations for cloud computing
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

BOARD AND CYBER SECURITY

“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
- Police are investigating a "significant and sustained cyber-attack" on the TalkTalk website, the UK company says, October 2015.
- Convention on Cybercrime, As of September 2015, 47 states have ratified the convention, seven states had signed the convention but not ratified it
- Danish Water Plants potential attack, November 2015
CYBER SECURITY FOR NUCLEAR POWER PLANTS

- Critical safety, security and emergency preparedness systems at nuclear energy facilities are isolated from the Internet.
- Protected by cyber security and physical security plans
- Nuclear power plants are designed to shut down safely
- Ordered to enhance security in several areas and subsequently codified the new requirements in 2009.
- New cyber security requirements. NRC-approved cyber security program.
- Mandatory, enforceable cyber security standards
- 2014 revised [cyber security rule](#) to align with the intent to protect public health and safety by preventing radiological sabotage.

Source: Nuclear Energy Institute, April 2015
TALKTALK ATTACK, OCTOBER 2015

• "TalkTalk constantly updates its systems to ensure they are as secure as possible against the rapidly evolving threat of cyber crime, impacting an increasing number of individuals and organisations," says TalkTalk CEO Dido Harding. "We take any threat to the security of our customers' data extremely seriously and we are taking all the necessary steps to understand what has happened here."
• Forensic analysis of the site confirms that the scale of the attack was much more limited than initially suspected.
• "Only" 4% of TalkTalk customers sensitive personal data at risk.
• Difficult decision to notify all our customers of the risk. We believe we had a responsibility to warn customers.

Do you expect a cyberattack to strike your organization in the next 12 months? (n = 1,549)

a. Yes.................................................................52%
b. No.................................................................24%
c. Unsure............................................................24%

Is your organization prepared for a sophisticated cyberattack? (n = 1,549)

a. Yes.................................................................40%
b. No.................................................................32%
c. Unsure............................................................28%

Source: ISACA 2015 IT Risk/Reward Barometer Europe Results, October 2015
CYBERATTACK – ISACA SURVEY

• When was your last Cyberattack/Breach:

  Greater than 18 months  11.03%
  12-18 months            11.03%
  6-12 months             8.09%
  2-6 months              14.71%
  Last 60 days            38.97%
  Never                   16.18%

Respondent: 126 participants.
Please take the poll under Session 211: Panel Discussion moderate by Rob Stroud

Source: Poll at EuroCacs/ISRM 2015, November 10, 2015
Geopolitical, macroeconomic, and cyber-related surprises have become almost routine. Source: IIA’s July 2015 “2015 Global Pulse of Internal Audit”

### The Board’s Perception of Cybersecurity Risks Over the Last One to Two Years

<table>
<thead>
<tr>
<th>Response</th>
<th>Chart</th>
<th>Frequency</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has been at a high level</td>
<td></td>
<td>8.5%</td>
<td>160</td>
</tr>
<tr>
<td>Increased significantly</td>
<td></td>
<td>18.7%</td>
<td>353</td>
</tr>
<tr>
<td>Increased</td>
<td></td>
<td>40.8%</td>
<td>772</td>
</tr>
<tr>
<td>Decreased</td>
<td></td>
<td>2.0%</td>
<td>38</td>
</tr>
<tr>
<td>Decreased significantly</td>
<td></td>
<td>1.1%</td>
<td>20</td>
</tr>
<tr>
<td>No change</td>
<td></td>
<td>28.9%</td>
<td>547</td>
</tr>
<tr>
<td>Not Answered</td>
<td></td>
<td></td>
<td>45</td>
</tr>
</tbody>
</table>

Source: IIA’s Audit Executive Center “Pulse of the Profession 2014“

Valid Responses: 1,890
Total Responses: 1,935
BOARD INVOLVEMENT DURING THE LAST FISCAL YEAR IN REGARD TO SPECIFIC ACTION OR REQUEST ON CYBERSECURITY PREPAREDNESS?

<table>
<thead>
<tr>
<th>Response</th>
<th>Chart</th>
<th>Frequency</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actively involved</td>
<td></td>
<td>14.1%</td>
<td>267</td>
</tr>
<tr>
<td>Involved</td>
<td></td>
<td>34.9%</td>
<td>662</td>
</tr>
<tr>
<td>Minimally involved</td>
<td></td>
<td>36.1%</td>
<td>686</td>
</tr>
<tr>
<td>Not sure of involvement</td>
<td></td>
<td>14.9%</td>
<td>283</td>
</tr>
<tr>
<td>Not Answered</td>
<td></td>
<td></td>
<td>37</td>
</tr>
</tbody>
</table>

Valid Responses 1,898
Total Responses 1,935

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

Rarely a day goes by without reference to new global threat or cyberattack.

Source: IIA’s Audit Executive Center “Pulse of the Profession 2014”

Source: IIA’s July 2015 “2015 Global Pulse of Internal Audit”
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 REGARDING CYBER SECURITY

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?
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
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

Applicability

• 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 – Appendix 62
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 nonexistent 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 – Appendix 63
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 on the 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

1st Line of Defense
- Management Controls
- Internal Control Measures

2nd Line of Defense
- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line of Defense
- Internal Audit

Governing Body/Board/Audit Committee
Senior Management

External Audit
Regulator
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)

<table>
<thead>
<tr>
<th></th>
<th>The benefit outweighs the risk.</th>
<th>The risk outweighs the benefit.</th>
<th>The risk and benefit are appropriately balanced.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public cloud</td>
<td>12%</td>
<td>68%</td>
<td>20%</td>
</tr>
<tr>
<td>Hybrid cloud</td>
<td>16%</td>
<td>40%</td>
<td>44%</td>
</tr>
<tr>
<td>Private cloud</td>
<td>57%</td>
<td>10%</td>
<td>33%</td>
</tr>
</tbody>
</table>

Source: IT Risk/Reward Barometer: Europe, 2012, ISACA (n=980)
# BUSINESS CHALLENGES TO CONSIDER

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incompatibility</td>
<td>Cloud services may not be compatible with the existing IT infrastructure or specific systems that must be integrated.</td>
</tr>
<tr>
<td>Uptime</td>
<td>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.</td>
</tr>
<tr>
<td>Performance</td>
<td>Multitenant models can degrade performance over time if capacity is not properly planned. Internet speed can also negatively impact performance.</td>
</tr>
<tr>
<td>Security</td>
<td>Cloud computing represents traditional and new risk that must be accounted for and mitigated accordingly (either by the CSP or the customer).</td>
</tr>
<tr>
<td>Compliance</td>
<td>The ubiquitous and abstract nature of the cloud can cause an enterprise’s transition from compliance to noncompliance without any notice.</td>
</tr>
<tr>
<td>Pay-as-you-go</td>
<td>The enterprise must implement controls to avoid overage charges incurred when systems stay connected after a demand spike is over.</td>
</tr>
<tr>
<td>Lock-in (hardware or vendor)</td>
<td>Customers may become locked into a specific technology or a specific cloud vendor, which can prevent portability.</td>
</tr>
<tr>
<td>Cloud consumerization</td>
<td>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.</td>
</tr>
<tr>
<td>Limited customization (Black Box)</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

ASSURANCE CONSIDERATIONS

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

# Positive and Negative Influences on Cloud Adoption and Innovation

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

Source: Cloud Computing Market Maturity Study Results, 2012, ISACA & CSA
## PERSPECTIVES ON SECURITY AND ASSURANCE COMPONENTS

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

<table>
<thead>
<tr>
<th>Security and Assurance Component</th>
<th>Overall Rank</th>
<th>Business Rank</th>
<th>Security Rank</th>
<th>Technology Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concerns for multitenancy</td>
<td>10</td>
<td>13</td>
<td>15</td>
<td>8</td>
</tr>
<tr>
<td>Information security</td>
<td>12</td>
<td>11</td>
<td>14</td>
<td>13</td>
</tr>
<tr>
<td>Testing and assurance</td>
<td>18</td>
<td>22</td>
<td>10</td>
<td>21</td>
</tr>
<tr>
<td>Data ownership/custodian responsibilities</td>
<td>22</td>
<td>23</td>
<td>23</td>
<td>19</td>
</tr>
<tr>
<td>International data privacy</td>
<td>25</td>
<td>25</td>
<td>27</td>
<td>25</td>
</tr>
</tbody>
</table>
ADDITIONAL RESOURCES

- 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 Global Economic Crime Survey
- Interpol and National Cyber Crime Investigation & Research
- Responding to Targeted Cyberattacks, 2014, ISACA & EY
- ISACA Knowledge Center: Cybersecurity Nexus
- 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 and C-suite
• Cloud computing are aligned to the enterprise strategy.
• Security and assurance.
• Keep updated via research and white paper
QUESTIONS

Associated Professor & Statsautøriseret Revisor
Hans Henrik Aabenhus Berthing
CGEIT | CRISC | CISA | CIA

Phone: +45 35 36 33 56 | Mobile +45 22 20 28 21
E-mail hhberthing@verifica.dk

Verifica Statsautøriseret Revisionsvirksomhed