10 Things Auditors Should Know

ABOUT CYBER SECURITY



1/ LEVERAGE EXISTING FRAMEWORKS/GUIDELINES

Auditors should consider mapping of the NIST "Framework for Improving Critical Infrastructure Cybersecurity" to ISO27001:2013 controls and COBIT 5 to reduce the scope of the audit, hence, making the audit more manageable.



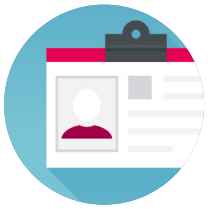
2/ CONSIDER FORTHCOMING LEGISLATION

Auditors should study how forthcoming and existing legislation like GDPR & PCI-DSS could potentially be incorporated into cyber security programs. Also, auditors need to understand the global regulatory environment and the differences that can exist between geographic regions (e.g., GDPR – PCI-DSS across the EU/US/China/Russia/India/Japan, etc.).



3/ ALL RISKS ARE SUBJECTIVE

To qualify as a "risk" a threat needs to be associated with a vulnerability that, if exploited, could negatively impact an information asset. If it does not, it is not a threat. Too many auditors worry about threats and vulnerabilities that pose no actual risk to an asset, prioritizing compliance over risk and wasting precious time and resources.



4/ USERS ARE (AND WILL ALWAYS BE) THE BIGGEST SECURITY RISK

Our industry is led by vendors and we continue to seek security through products (firewalls, IDS/IPS, encryption, anti-malware, DLP, etc.). We invest in product before people while real and measurable results can be achieved by investing in information security awareness. To contribute tangible results, auditors should prioritize people over product. Cyber security education is the silver bullet.



5/ BASIC INFORMATION SECURITY CONTROLS STILL HOLD TRUE

As part of overall security (including cyber security), these controls provide a valid baseline of security controls that help enforce security-in-depth (e.g., physical & logical access controls, application of "principle of least privilege").



6/ NEED A CYBER INCIDENT RESPONSE POLICY AND PLAN THAT IS FULLY TESTED

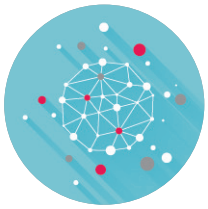
Auditors need to assess whether a proper crisis management and communication plan is in place and clearly communicated and tested as appropriate. This should enable sufficient business continuity in event of a cyber security breach. Crisis management should include incident response and forensics, where warranted. Proactive monitoring and detection (with automated tools) should be in place.

For more information, go to ***isaca.org/auditing-cyber-security.***

© 2016 ISACA. All rights reserved.

10 Things Auditors Should Know

ABOUT CYBER SECURITY



7/ CYBER SECURITY STRATEGY NEEDS TO BE AGILE – LANDSCAPE IS "MUTATING"

Strategy needs to be adaptable and scalable to handle new attack methods, such as ransomware/BYOD risk/cloud-3rd party risk/social media etc. Auditors need to be aware that this is an area that is constantly changing–cannot assume that what currently keeps your IT environment secure will continue to remain secure indefinitely.



8/ CYBER SECURITY AWARENESS DEPENDS ON THE RIGHT TRAINING

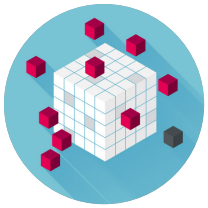
Employees need sufficient and timely education and training to help combat the ever-changing cyber security threat. Security needs to be interwoven into the fabric on an organization. One off/tick box exercises are not sufficient. For example:

- Do employees actually understand implications of a cyber security breach?
- Has any thought been given to insider threats from a cyber security perspective?
- Is there clear guidance on use of social media/shadow IT solutions/BYOD/how to respond to a phishing or ransomware attack?
- Are employees rewarded/praised for promoting security in an organization — are they incentivized?



9/ EVERYTHING IS CONNECTED TO EVERYTHING

The primary function and objective of any cyber device is connectivity. Devices are like climbers roped together on the side of a mountain — if one falls it can bring down anything connected to it. The Target hack (through an HVAC supplier connection) clearly demonstrates the need for a holistic cyber security view. With the arrival of the IoT, it's imperative that auditors understand and address the bigger picture.



10/ BE AWARE OF CREDENTIAL THEFT TECHNIQUES

Auditors should have knowledge of credential theft attack techniques (e.g. pass-the-hash, key logging, passing tickets, token impersonation, and man-in-the-middle attacks). Typically, the Pass-the-Hash (PtH) attack and other credential theft and reuse types of attack use an iterative two-stage process. First, an attacker captures account logon credentials on one computer, and then uses those captured credentials to authenticate to other computers over the network.

ISACA®

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

DISCLAIMER

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

RESERVATION OF RIGHTS

© 2016 ISACA. All rights reserved.

For more information, go to ***isaca.org/auditing-cyber-security.***

© 2016 ISACA. All rights reserved.