Lessons From History

So, in case you have been living in a cave somewhere, ISACA® is 50—a significant historical milestone. History, we are taught, can often be better understood through artifacts, “An object made by a human being, typically one of cultural or historical interest.”[1] One of the most significant artifacts to have been created in ISACA’s history is, undoubtedly, COBIT®. To me, it represents a large part of the collective knowledge of ISACA volunteers—knowledge that was acquired both before and after its first release in 1996.

Of course, history is important because we can learn from it. Certainly, that humans do not learn very much from the lessons of history is the most important of all the lessons that history has to teach.[2] In the world of IT audit, we learn from history in the form of case studies such as data breaches. In fact, in December 2018, the US House of Representatives Committee on Oversight and Government Reform produced a report on the Equifax data breach.[3] The report contains a section titled, “Specific Points of Failure,” from which I believe learning can be found. Could COBIT have helped identify any of these issues?

Equifax IT Management Structure Lacked Accountability and Coordination

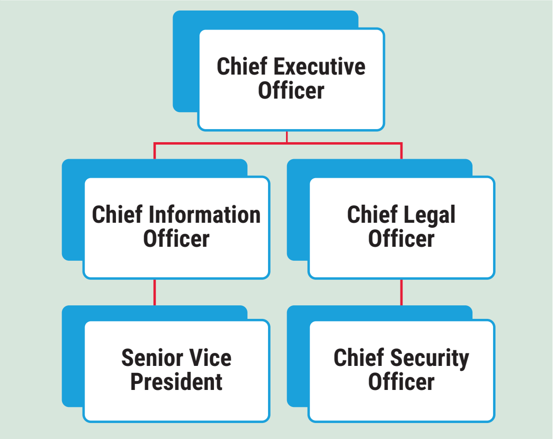
In 2005, as working relationships between senior executives became strained, Equifax reorganized its IT organization structure (**figure 1**) so that the chief security officer (CSO), who was responsible for IT security, reported to the chief legal officer (CLO) rather than the chief information officer (CIO). The company did not revert the IT organizational structure back to its original form (where the CSO reported to the CIO) following new appointees despite there being multiple discussions to do so.

The functional result of the CIO/CSO structure meant IT operational and security responsibilities were split, creating an accountability gap. At the time of the breach, the organizational structure did not facilitate a strong CIO and CSO partnership.[4]

Depending on the organizational reporting structure an organization adopts, the CSO and CIO roles can be conflicting or complementary. At Equifax, the IT and security organizations were siloed, meaning information rarely flowed from one group to the other. Collaboration between IT and security mostly occurred when required, such as when security needed IT to authorize a change on the network. Communication and coordination between these groups was often inconsistent and ineffective.

One example of the lack of IT-security coordination was that multiple and incomplete software inventory lists were kept independently by each group. Both IT and security rely on accurate inventory lists to operate, patch and monitor the

Figure 1—Equifax IT Organizational Structure (2013 - September 2017)



Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, CPTE, DipFM, FIP, ITIL Foundation, Six Sigma Green Belt

Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a past member of ISACA’s CGEIT® Exam Item Development Working Group. He is the topic leader for the Audit and Assurance discussions in the ISACA Online Forums. Cooke supported the update of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for the development of ISACA’s CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*), or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2Wbf3Nb

organization's IT systems. In a more collaborative environment, these lists would be merged into a single master document with both teams working together to complete the inventory.[5]

In addition, the organization did not prioritize cybersecurity. Quarterly senior leadership team meetings were held where IT security was just one of the many topics discussed. Further, the CSO did not regularly attend these meetings because the CSO was not considered part of the senior leadership team. As a result of this, the chief executive officer (CEO) was not receiving timely information on Equifax's security posture. The information he did receive was presented by the chief legal officer (CLO), who did not have any background in IT or security.

Clearly this was not a tenable situation, but how could COBIT have helped? COBIT has defined the mandate, operating principles, span of control and authority level of the chief information security officer (CISO) (**figure 2**).[6] COBIT does indicate that, depending on a variety factors within the enterprise, the CISO may report to the CEO, chief operating officer (COO), CIO, chief risk officer (CRO) or other senior executive management,[7] however, it also specifies the CISO as the liaison between executive management and the information security program.[8] This, in my opinion, can be done through the CIO, however, ideally, the CISO should report to the CEO.[9] In February 2018, Equifax announced a revised reporting structure elevating the (now renamed) CISO to directly report to the CEO.[10]

Equifax Had Serious Gaps Between IT Policy Development and Execution

At the time of the breach, Equifax's internal IT management process failed to establish clear lines of accountability for developing IT security policies and executing these policies.[11]

The disconnect between policy development and execution was especially pronounced with respect to the patch management policy. This policy defined roles and responsibilities, and established guidelines for the patching process. The policy designated two employees to lead implementation—a policy manager and a senior leadership team owner. The responsibility of the policy manager was to ensure that all of the work

Figure 2—CISO: Mandate, Operating Principles, Span of Control and Authority Level

Area	Characteristic
Mandate	The overall responsibility of the enterprise information security programme
Operating principles	Depending on a variety factors within the enterprise, the CISO may report to the CEO, COO, CIO, CRO or other senior executive management. The CISO is the liaison between executive management and the information security programme. The CISO should also communicate and co-ordinate closely with key business stakeholders to address information protection needs. The CISO must: • Have an accurate understanding of the business strategic vision • Be an effective communicator • Be adept at building effective relationships with business leaders • Be able to translate business objectives into information security requirements
Span of control	The CISO is responsible for: • Establishing and maintaining an information security management system (ISMS) • Defining and managing an information security risk treatment plan • Monitoring and reviewing the ISMS
Authority level/decision rights	The CISO is responsible for implementing and maintaining the information security strategy. Accountability (and sign-off of important decisions) resides in the function to which the CISO reports, for example, senior executive management team member or the ISSC.
Delegation rights	The CISO should delegate tasks to information security managers and business people.
Escalation path	The CISO should escalate key information risk-related issues to his/her direct supervisor and/or the ISSC.

Source: ISACA®, *COBIT® 5 for Information Security*, USA, 2012. Reprinted with permission.

they needed to do was tracked, while the senior leadership team owner's role was to ensure that the organization conformed to the policy.

The patch management policy also identified the roles and responsibilities for various individuals within their portfolios. The business owner was informed of the need to patch and was responsible for approving downtime so the patch could be applied. The system owner was responsible for applying the patch, and the application owner was then responsible for ensuring the patch was applied correctly. While roles and responsibilities were defined in the policy, there were no official designees for these roles. Again, this was not an acceptable situation.

COBIT® 2019 process Deliver, Service and Support (DSS) includes the management practice DSS05.01 *Protect against malicious software*, which requires an organization to implement and maintain preventive detective and corrective measures in place (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).[12]

In addition, COBIT 2019 defines who is responsible and accountable (**figure 3**) for each of its key management practices. Clearly, the message here is that these roles should be mapped to named individuals in each of our enterprises.

Also noteworthy was the fact that internal audit had reported issues with the patching process. These included the failure to patch or remediate vulnerabilities in a timely manner. The lesson here is clearly to follow up on audit recommendations through to their implementation.[13]

Equifax Ran Business-Critical Systems on Legacy IT With Documented Security Risks

Equifax faced increased security risk due, in part, to its complex legacy IT environment. Legacy technology is both a security issue and a hindrance to innovation, and legacy systems are tough to secure because they are often extremely difficult to patch, monitor or upgrade. Equifax ran a number of its business-critical systems on legacy infrastructure, including the system compromised by attackers during the 2017 data breach.[14]

The use of legacy technologies and applications resulted in a dwindling number of employees with knowledge of how to operate and maintain the aging system. For example, Equifax did not have a comprehensive picture of the software used within the application. This was a key issue, as the patch management policy relied on its employees knowing the source and version of all software running on a certain application in order to manually initiate the patching process.

Equifax recognized the risk posed by continued operation of its legacy IT systems, had documented some security risk factors and even planned an upgrade, however, it failed to move quickly enough, resulting in the breach of the system.

Again, COBIT has documented these risk scenarios. Build, Acquire and Implement (BAI) BAI03.10

Figure 3—COBIT DSS05.01 Protect Against Malware RACI Chart

B. Component: Organizational Structures								
Key Management Practice	**Chief Information Officer**	**Chief Information Security Officer**	**Business Process Owners**	**Head Human Resources**	**Head Development**	**Head IT Operations**	**Information Security Manager**	**Privacy Officer**
DSS05.01 Protect against malicious software.		A	R	R	R	R	R	

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018. Reprinted with permission.

Maintain solutions requires an enterprise to develop and execute on a plan for the maintenance of solution and infrastructure components, and to include periodic reviews against business needs and operational requirements. Organizations should also develop and execute on a plan for the maintenance of solution components that includes periodic reviews against business needs and operational requirements such as patch management, upgrade strategies, risk, vulnerabilities assessment and security requirements (**figure 4**).

Conclusion

It has not been my intention to single out Equifax and point fingers. Certainly, let he or she who is without security vulnerabilities cast the first aspersion. However, in this historical year for ISACA, I do believe that it is important that we learn from what is an excellent report from the US House of Representatives. ISACA's artifacts, especially COBIT, can aid us in doing so and ensure that, in turn, history is kind to us. "Those who cannot remember the past are condemned to repeat it."[15]

Endnotes

1. Oxford Dictionary, "Artifact," *https://en.oxforddictionaries.com/definition/artefact*
2. Huxley, A.; *Collected Essays*, Harper and Brothers, USA, 1958
3. US House of Representatives Committee on Oversight and Government Reform, *The Equifax Data Breach*, Majority Staff Report, 115th Congress, December 2018, *https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf*
4. *Ibid*., p. 58
5. *Ibid*., p. 61
6. ISACA®, COBIT® 5, USA, 2012, *www.isaca.org/COBIT*
7. *Ibid*.
8. *Ibid*.
9. Putrus, R.; "The Role of the CISO and the Digital Security Landscape," *ISACA® Journal*, vol. 2, 2019, *https://www.isaca.org/Journal/archives*
10. *Op cit The Equifax Data Breach*, p. 60
11. *Ibid*., p. 61
12. ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx*
13. Cooke, I.; "Enhancing the Audit Follow-up Process Using COBIT 5," *ISACA Journal*, vol. 6, 2016, *https://www.isaca.org/archives*
14. *Op cit The Equifax Data Breach*, p. 71
15. Santayana, G.; *The Life of Reason: Reason in Common Sense,* Scribner's, USA, 1905, *https://www.iep.utm.edu/santayan/*

Figure 4—COBIT DSS05.01—Protect Against Malware, Organizational Structures

BAI03.10 Maintain solutions. Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	a. Number of demands for maintenance that are not satisfied b. Duration of demands for maintenance that are satisfied and that go unsatisfied

Activities	Capability Level
1. Develop and execute a plan for the maintenance of solution components. Include periodic reviews against business needs and operational requirements such as patch management, upgrade strategies, risk, privacy, vulnerabilities assessment and security requirements.	2
2. Assess the significance of a proposed maintenance activity on current solution design, functionality and/or business processes. Consider risk, user impact and resource availability. Ensure that business process owners understand the effect of designating changes as maintenance.	3
3. In the event of major changes to existing solutions that result in significant change in current designs and/or functionality and/or business processes, follow the development process used for new systems. For maintenance updates, use the change management process.	
4. Ensure that the pattern and volume of maintenance activities are analyzed periodically for abnormal trends that indicate underlying quality or performance problems, cost/benefit of major upgrade, or replacement in lieu of maintenance.	4

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018. Reprinted with permission.