# Logical Security Architecture (Designer's view): Equifax case study

Daniel Cordeiro Marques

University of San Diego

CSOL-520-03-FA20 - Secure Systems Architecture

Dr. Michelle Moore

December 14, 2020

## Table of Contents

Logical Security Architecture (Designer's view): Equifax case study

Equifax is one of the primary credit bureaus serving the United States. As a victim of a data breach in 2017 and a company that continues to expand its service offerings to aggregate and process personally identifiable information, Equifax can benefit from an effective security architecture. This paper describes a mock logical architecture for Equifax, based on the SABSA framework (Sherwood et al., 2005) and publicly available information. Specifically, this work leverages Equifax's 2019 annual report (Equifax, 2020) to establish risks and business drivers and the U. S. Government Accountability Office (GAO)'s report to derive a gap analysis (Marinos & Clements, 2018).

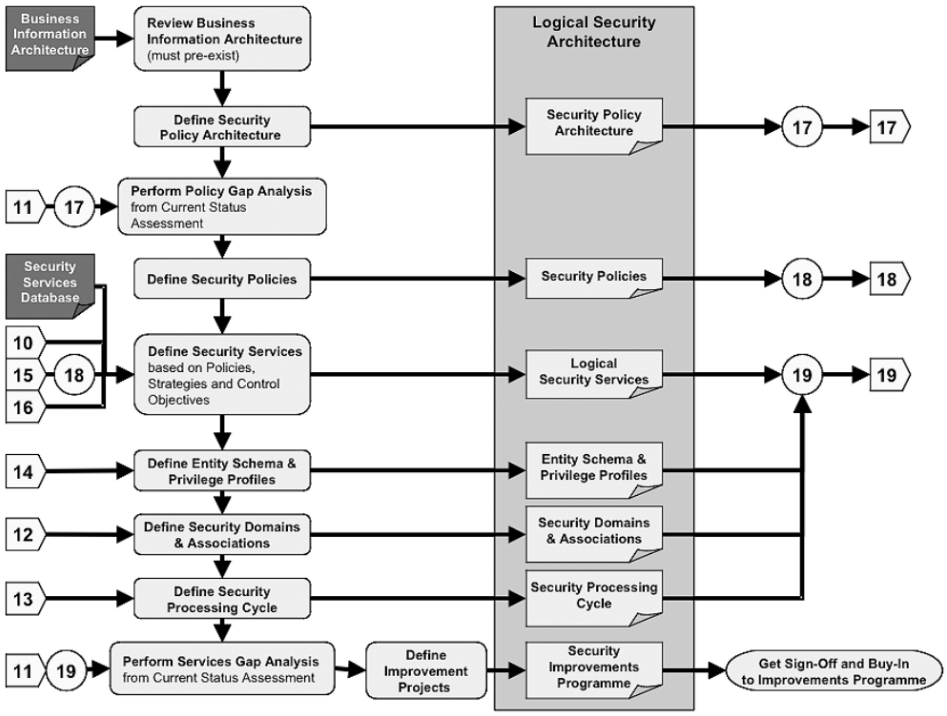
## Information Required to Created the Logical Architecture

As a layered model, designing a logical security architecture following the SABSA framework depends on documentation created by previous layers - mainly an "agreed, signed off, conceptual security architecture, based upon an agreed, signed off contextual security architecture" (Sherwood et al., 2005, p. 118). Figure 1 expresses this dependency, with the connectors resulting from deliverables of the Conceptual Security Architecture as identified below (Sherwood et al., 2005, p. 114):

11. Assessment of the current security status of the enterprise
12. Security domain model
13. Security Related Lifetimes & Deadlines
14. Security Entity Model & Trust Framework
15. Security Strategies and Architectural Layering
16. Individual Strategy break-out documents

**Figure 1**.

*Information Dependencies to Develop the Logical Security Architecture (Sherwood et al., 2005, p. 119, Figure 7-9)*




This section makes assumptions to develop a mock logical security architecture as this information is not readily available.

**Business Drivers, Risks, and Control Objectives**

Business drivers, risks, and control objectives are not established during the conceptual security architecture but make an essential part of developing logical security architectures. The architect typically obtains these details from discussions with the company's stakeholders, which were not available for interviews while producing this work; nevertheless, these details can be derived from publicly available information, primarily the company's annual report. Table 1

enumerates five high-level business drivers, risks, and control objectives from analyzing Equifax (2020).

**Table 1**.

*The high-level business model for Equifax based on Equifax (2020)*

| Business Driver | Business Attributes | Business requirement | Control Objectives |
|---|---|---|---|
| Become an industry leader in data security | Protected, Accountable, Recoverable, Monitored, Assurable, Access-controlled, confidential. | Build a culture where data security and risk management drives all decisions, and information is protected from unauthorized access. | CO1. Establish effective security controls to safeguard all customer data during its lifecycle. |
| Deliver market-leading capabilities to clients | Accessible, Consistent, Protected, Reliable, Responsive, Timely, Usable, Controlled, Cost-effective, Supportable, Available, Recoverable. | Expand the portfolio of cloud-native services, increasing the ability to quickly deploy new services that clients find easy to integrate and deploy. | CO2. Establish adequate security controls to safeguard the cloud-based services and associated data. |
| Become a leader in data and analytics | Protected, Accountable, Recoverable, Monitored, Assurable, Access-controlled, confidential. | Data should be acquired from multiple sources and processed accurately and timely. Client access to data should be simplified. | CO1. Establish effective security controls to ensure the integrity of the information during its lifecycle. |
| Improve the consumer user experience | Accessible, Consistent, Current, Protected, Reliable, Responsive, Timely, Usable, Controlled, Cost-effective, Supportable, Available, Inter-operable. | Security features should not impact the consumer experience in implementing and integrating services and accessing required data. | CO3. Establish consistent and easy-to-use authentication procedures to access customer information. |
| Promote a culture of innovation | Accessible, Consistent, Current, Protected, Reliable, Responsive, Timely, Usable, Controlled, Cost-effective, Supportable, Available, Inter-operable. | Security features should not impact the company's ability to innovate and to deploy new services quickly. | CO4. Establish consistent security controls that support the quick deployment of customer-facing services while safeguarding information and maintaining compliance with applicable law |

**Table 1 (*cont.*)**

*The high-level business model for Equifax based on Equifax (2020)*

| Business Driver | Business Attributes | Business requirement | Control Objectives |
|---|---|---|---|
| Compliance with data-privacy regulation | Protected, Accountable, Recoverable, Monitored, Assurable, Access-controlled, confidential. | Equifax must comply with data protection and privacy legislation from different countries. | CO5. Establish controls to ensure compliance with applicable data protection and privacy laws |

A documented business information architecture is critical to understanding how the logical assets correlate and support the business requirements and the control objectives.

**Business Information Architecture (BIA)**

The BIA is the "logical representation of the real business" (Sherwood et al., 2005, p. 290). It describes the relationship between different systems, information flow, data structures, classification, and associations. The security architect is not responsible for developing the BIA. Regarding Equifax, this information was not available for this work; therefore, the Consumer Financial Protection Bureau (2012) served as a reference. The document outlines technical processes and information schema for credit bureaus (including Equifax).

**Security Strategies, Architectural Layering, and Individual Break-out Documents**

The Conceptual Architecture should offer the designer a clear direction for the security strategy, including the different layers and supporting security services. This paper considers a zero-trust architecture (Rose et al., 2020) as the primary model for Equifax's security strategies and architectural layers since this information is not publicly available. Companies that process sensitive customer information benefit significantly from segmentation strategies; the financial

industry frequently implements this approach to comply with standards and data privacy legislation.

**Security Entity Model and Trust Framework**

As part of the Conceptual Architecture, the architect defines a security entity model describing the entities that can take actions in the environment, their relationship, and their trust. Consumer Financial Protection Bureau (2012) provides insights into distinct entities involved in transactions management by Equifax and should be used combined with the zero-trust philosophy to restrict access only to the necessary functions.

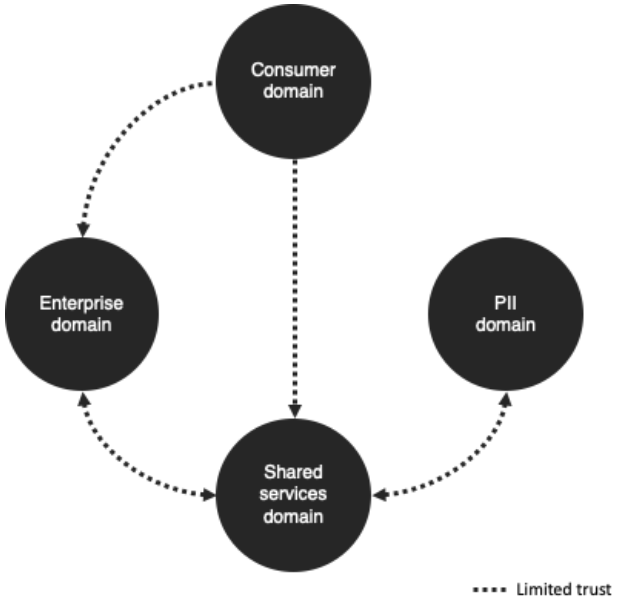
**Security Domain Model**

Sherwood et al. (2005) defines security domains as "a set of security elements subject to a common security policy and enforced by a single policy authority" (p. 266). Figure 2 represents a high-level security domain model based on the honeycomb model, derived from analyzing Equifax (2020), Consumer Financial Protection Bureau (2012), and Marinos & Clements (2018).

These domains should follow the zero-trust model. Therefore services and connectivity should be limited to a minimum.

**Figure 2**.

*The high-level security domain model for Equifax.*




**Security-Related Lifetime and Deadlines**

As Equifax demonstrated concerts with applicable data privacy and protection laws, the security strategy must account for data retention times. Additionally, the architecture must address the timeline between registration and revocation of access for enterprise users and consumers. Finally, the designed policies must address the digital certificate's lifecycle.

**Assessment of Current State of Security**

Since Equifax was not available to assess potential security gaps, this paper considers the analysis resulting from the Equifax 2017 security incident as an assessment of their current state. In particular, Marinos & Clements (2018) and Wang & Johnson (2018) provide detailed information regarding the gaps exploited by the attackers and insights on the company's incident response process. In particular, the logical security strategy must address four gaps:

**Deficient patch management strategy.** Attackers exploited a server affected by a well-known vulnerability to gain initial access to the network.

**Lack of segmentation between sensitive systems and accounts.** Attackers reused credentials and pivoted through systems without any barriers to separate these assets.

**Deficient data protection strategy.** Threat agents compromised accounts and customer information found unencrypted in servers and databases.

**Deficient network monitoring.** The attackers persisted in the network for over a month and exfiltrated millions of records without detection.

The mock security architecture designed in this paper aims to address these issues.

## A Mock Logical Security Architecture for Equifax

The logical security architecture will define the requirements for Equifax to address the security concerns identified in the gap analysis and to realize the vision created by the conceptual and contextual architectures. The mock security architecture proposed by this paper focuses on three elements: flexibility to deploy new services to customers, customer data protection, and compliance with privacy regulation. It starts with the definition of a security policy architecture.

### Security Policy Architecture

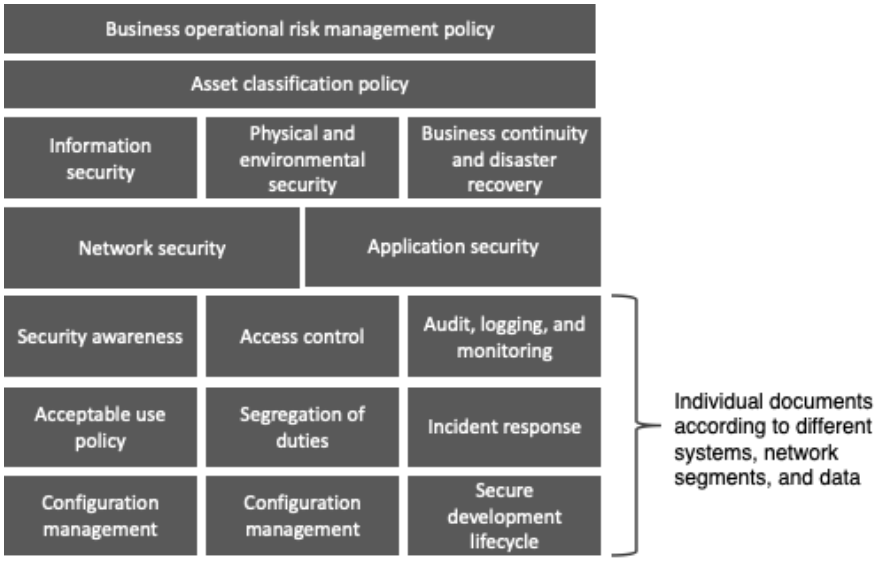
The security policy's scope is limited: it covers only the systems, data, and users under Equidax's responsibility. It should not make provisions regarding customer's systems, except in terms of an acceptable use policy for the information provided by Equifax.

First, as noted in Equifax (2020, p. 3), one of the company's business requirements is to have risk management at the core of their business decisions. Therefore, the Business Operational Risk Management Policy should be at the top of the security policy architecture. In

the next layer, the asset classification policy establishes how to classify systems, data, and other entities according to the impact they can cause to the business requirements if they are compromised, and all subsequent layers should reference it. The following layer approaches the overall security policies for networking and applications. Lastly, individual security policies cover the different services provided by Equifax and their associated assets. Figure 3 illustrates the proposed mock security policy architecture.

**Figure 3**.

*The mock security policy architecture for Equifax.*




**Security Policies**

All security policies must be written in a concise and straightforward language (Bacik, 2008, p. 25), referencing elements from the applicable upper layer in the security policy architecture, and communicated to all entities involved in the process. The documentation for each policy must address the following: scope, high-level statement of goals, expected behavior, and sanctions in case of non-compliance. These policies must be reviewed annually to ensure

their alignment with the overall business strategy. Taking into consideration the gap analysis established previously, Equifax must review or develop the following policies in particular:

**Asset classification policy.** This policy establishes the requirements to classify data, systems, and other assets in terms of their criticality, business value, and sensitivity in case a security event occurs. This policy must make provisions on how the organization handles the assets according to its classification.

**Network security policy.** This policy determines Equifax's requirements to manage networks and control information flow through the environment. The policy must make provisions to ensure availability, integrity, and confidentiality of assets according to their classification, without rendering the company's ability to deploy new services quickly. It must also ensure network segmentation according to the zero-trust model.

**Access control policy.** This policy establishes the requirements to access Equifax's networks, applications, data, and the cloud environment. It must cover both internal users and customer access to service, including the lifecycle of subscriptions and user accounts. The policy must also address compliance with applicable law and access controls in the cloud environment.

**Configuration management policy.** This policy determines the requirements for secure configuration of assets, including change management, separation of development, testing and production environments, baseline definition, patch and vulnerability management, and periodic configuration audits.

**Encryption and digital certification management policy.** This policy defines the data encryption requirements according to the data classification. For instance, systems must encrypt customer information and credential material at least while in transit and at rest. It must also

make provisions on encryption key management, and the management of the digital certificate lifecycle, including issuance, expiration, and renewal. Finally, the policy should also address audit controls to ensure the efficiency of encryption and digital certification processes.

**Secure development lifecycle policy.** This policy establishes requirements for the development, deployment, and maintenance of software according to the classification of data managed by the system. It must include provisions regarding outsourced development, security and acceptance testing, and change management.

Logical security services driven by the business attribute profile and the security strategy (Sherwood et al., 2005, p. 294) carry the enforcement of policies.

**Logical Security Services**

To support the policies and control objectives established by the conceptual architecture while addressing the gaps identified, Equifax must improve the following security services:

**Environmental security (Control objectives: CO1, CO4, CO5).** This service must offer mechanisms to protect both the physical and the logical domains, establishing controls that protect systems and data according to their classification. This service should offer physical security mechanisms to safeguard facilities against natural disasters, accidents, and attackers.

**Logical access control (Control objectives: CO1, CO2, CO3, CO4, CO5).** Equifax must control access to systems and databases, creating different logical segments according to the asset classification. The physical services must grant access on a per-session basis according to the privilege of the entity requesting the resource. Furthermore, this service should consider geographically dispersed users and restrictions associated with their locality. This service must apply micro-segmentation to dynamically grant access to resources based on policy and the

entities' roles. Finally, this service must offer mechanisms to control access to Equifax's cloud environment, including data handled by these systems.

**Stored data confidentiality (Control objectives: CO1, CO2, CO4, CO5).** Encryption must be applied to sensitive data while at rest and in transit. Specifically, personally identifiable information (PII) and credentials should always be encrypted in case an attacker compromises the systems handling the data. This service must consider data handled by Equifax's cloud-based systems.

**Stored data integrity protection (Control objectives: CO1, CO2, CO4, CO5).** This service must implement controls to ensure consumer data handled in Equifax's systems is not modified or deleted by unauthorized parties. Systems must implement message integrity mechanisms to data at rest, in transit, and in motion. This service must also provide mechanisms to safeguard data handled by Equifax's cloud-based systems.

**Security monitoring (Control objectives: CO1, CO2, CO5).** Entities must be monitored for compliance with security policies and unexpected events. Agents must report to a centralized service that must offer the capability of cross-referencing data and provide sufficient structured information to aid an analyst in performing root-cause analysis. For instance, Equifax must create mechanisms to identify and report expired digital certificates, users performing suspicious activities, and systems missing patches or not following the security baseline.

**Security audits (Control objectives: CO1, CO2, CO5).** This service must collect audit information from entities for auditing purposes. Systems must record logs into a centralized service periodically, including access control and activity events. Systems must allow for manual collection of audit records for further examination. At a minimum, these logs must identify the

following details regarding an event: type, date and time, location, source, outcome, and entities associated with the event.

**Entity Schema and Privilege Profiles**

Sherwood et al. (2005) define a schema as "a set of rules that determines what data can be stored in a database or directory" (p. 320). Companies like Equifax typically leverage Microsoft's Active Directory (AD) to provide this service; AD helps to maintain the integrity of objects and their attributes and enforces authentication and authorization according to the entity's roles. Equifax must ensure the following high-level roles exist and are being enforced in the environment:

**Enterprise user.** These users should only have access to information on their role in the enterprise environment. They should not access PII unless needed.

**Administrators - Enterprise systems.** These administrators have privileged access to enterprise systems, but not to systems handling PII.

**Administrators - PII systems.** These administrators have privileged access to PII-related systems, but not to the enterprise systems.

**Consumer.** Consumers must only have access to their information or data assigned to them. Access to enterprise systems must not be allowed.

Administrators might assume the role of enterprise users, enterprise system administrators, and PII system administrators. However, they must use different accounts to perform activities associated with each role.

**Security Domains and Associations**

Security domains and associations define the entities that will be covered by the same security policy and how these security policies interact with each other. Equifax can be divided into four primary security domains:

**Enterprise domain.** The enterprise domain encompasses entities that support the core business functions (for instance, finance, HR, and investor relations). This domain encompasses the corporate network, systems, and employees that do not handle consumer data, and partners offering services to Equifax. There must be no interaction between this domain and the PII domain.

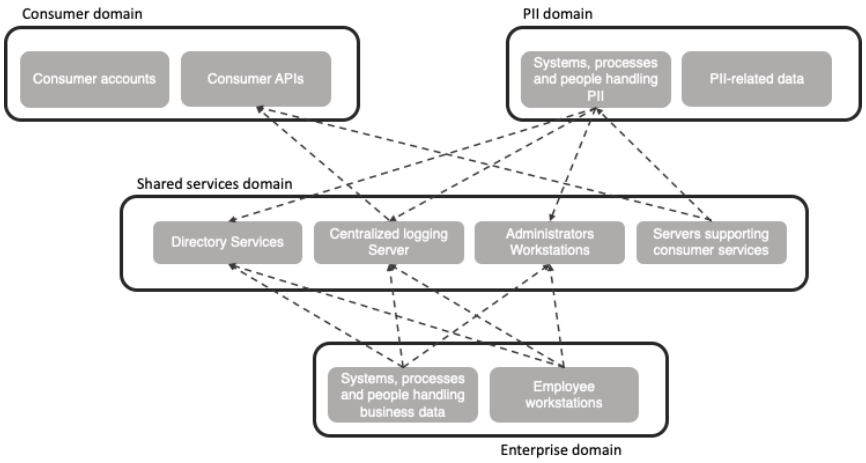
**Shared services domain.** This domain covers services that are common to all four domains, including directory services, logging services, and the workstations of system administrators. Trust between this domain and the others should be limited to services that are required to perform the intended function. Specific policies must exist to govern access controls and segmentation between this domain and the other three domains.

**PII domain.** The PII domain encloses entities handling PII, and PII data. The middleware in the shared services domain offers access to these systems, and no interaction should exist between the consumer and the enterprise domain. Policies to govern the use and administration of entities should consider their interaction with the shared services domain.

These domains enforce a consistent security policy between enterprise and nonenteprise infrastructure, with no inherent trust, and no implicit trust in the enterprise network (Rose et al., 2020). Figure 4 provides a high-level illustration of the security domains and their associations.

**Figure 4**.

*The security domains and their associations.*




**Security Processing Cycle**

The security processing cycle security aggregates security-related processes and their logical flow. Based on the control objectives, gap analysis, and security policies, the following processes are critical for the Equifax security architecture:

**Privileged account management.** A user receives a privileged account only after going through an approval process. Users with privileged accounts must change their passwords monthly. An automated system must disable accounts unused for more than 60 days. Privileged access to PII systems should occur for a limited time.

**Digital certificate management.** The certificates renewal process must be started at least two months before the certificate expires.

**Configuration management.** Equifax must perform daily automated vulnerability scans and weekly automated compliance scans. An analyst should perform a manual review of configurations at least once a year. The output of these actions must start a process to address any findings.

**High-level Security Improvement Program Roadmap**

Based on the gap analysis, this paper proposes a high-level three-phased security improvement program covering short-term projects that implement the defined logical security architecture. During each phase, the senior management must be involved to gain visibility of changes and associated benefits. Figure 5 illustrates this roadmap.

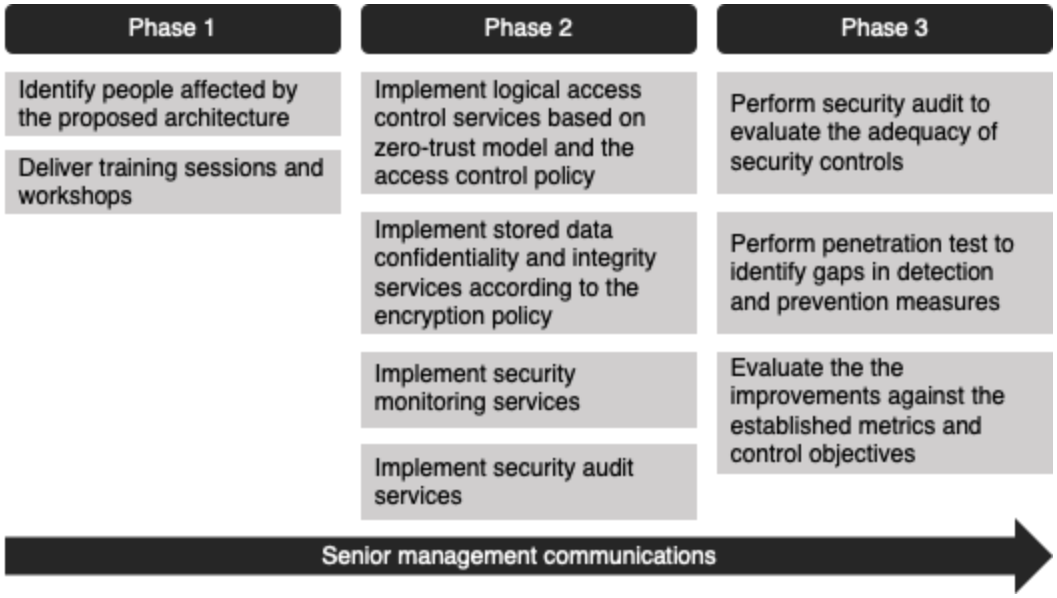
**Phase 1 - Educate.** The first phase focuses on educating stakeholders on the proposed improvement plan. This phase must engage all teams affected by the new policies and provide mechanisms to implement these policies with minimal impact.

**Phase 2 - Security service review and implementation.** Based on the findings from Marinos & Clements (2018) and Wang & Johnson (2018), begin the review and implementation of the following security services: logical access control, stored data confidentiality, stored data integrity protection, and security monitoring. This phase should start with a full scan of the network to identify sensitive information stored unencrypted, followed by the identification of gaps in the network segmentation.

**Phase 3 - Audit.** To demonstrate the improvements derived from the past two phases, the security team must test the security services implementation and compare the results with the gap analysis. First, a manual audit of the services against the policies will provide insights into the efficacy of the controls in place. Next, a penetration test can illustrate how the adopted controls withstand an attacker in the Equifax environment.

**Figure 5**.

*The security improvements roadmap.*



## References

Bacik, S. (2008). *Building an effective information security policy architecture*. CRC Press.

Consumer Financial Protection Bureau. (2012). *Key dimensions and processes in the U.S. credit reporting system: A review of how the nation's largest credit bureaus manage consumer data*. https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf

Equifax. (2020). *The New Equifax: Investing in cloud technology to drive innovation and growth* [2019 Annual Report]. https://investor.equifax.com/financial-information/annual-reports-and-proxy-statements

Marinos, N., & Clements, M. (Eds.). (2018). *Data protection: Actions taken by Equifax and federal agencies in response to the 2017 breach* [GAO-18-559]. U. S. Government Accountability Office. https://www.gao.gov/products/GAO-18-559

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* [NIST Special Publication 800-207]. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture: A business-driven approach* (1st ed.). CRC Press.

Wang, P., & Johnson, C. (2018). Cybersecurity incident handling: A case study of the Equifax data breach. *Issues in Information Systems*, *19*(3), 150-159. https://doi.org/10.48009/3_iis_2018_150-159