Security Audit Brief

MK Agents

Purpose

The purpose of a security audit is to identify and determine the severity of security issues that are undiscovered or unaccounted for. For this reason, security audits are essential for businesses, as they can help to identify issues that, if left undiscovered, could impact the trust and profit margins of the business. This document aims to outline the impacts to organisational security, then the roles of the stakeholders and finally how organisational policy can be adjusted.

Impacts & Effects

As mentioned above, the core purpose of a security audit is to identify and resolve issues with security and policy. Because of this, the impact of security audits can be both positive and significant; large organisational changes to combat security risks can be costly and time consuming. However, these changes will be a net positive over time, resulting in issues being resolved and risks being managed. The five key impacts are:

> 1. Improved consumer trust and business reputation
> 2. Increased organisational effectiveness
> 3. Protection of data and systems across the business
> 4. Discovery of issues within security policy
> 5. Compliance with regulations and laws

(Dube, 2011) (Maxwell, 2014)

To expand upon this, customer trust and reputation relies upon good data security, with large scale issues becoming much more common over the years (Reklaitis, 2018). Consumer trust is impacted on a huge scale because of these breaches (Greenlow, 2019). Negating the risk of damage to consumer trust, along with reputation, is a hugely important part of why security audits should take place, especially if user data is being stored or processed. Users prefer trustworthy businesses and services, with Google searches of businesses with negative articles on the first page lowers the amount of business they receive by ~20% (Hinckley, 2015).

Organisational security policy can affect the performance of both employees and the business overall. Setbacks caused by security issues can delay business operations at many different scales. Devices being damaged or destroyed by a lack of policy on found USB sticks could impact individual employees (Taylor, 2018). On the other end of the scale, physical or virtual breaches can result in the requirement to correct the issue, both the cause and the resulting effects. This can lower productivity because of the potential requirements for the solution taking up time and money.

Data protection and storage policy could have huge impacts, with large scale breaches involving potentially millions of users having personally identifiable

information being leaked, with billions of records being breached in 2019 alone (Henriquez, 2019). This frequency and severity of data breaches means there's a lot of risk involved with data storage and handling, impacting how business is conducted and how projects are assessed for risks.

Role of Stakeholders in Implementation

Stakeholders are parties inside or outside of a company that are involved with the operations of the company, whether directly or indirectly. Some stakeholders, such as an employee or a CEO, have a direct connection to the operations of the business. Others have an indirect connection, such as customers and investors. In all these cases they fit the definition of a stakeholder by being involved in the business in some way (Anderson, 2019).

Identifying the stakeholders involved in a security policy and, by extension, an update to an information security policy (ISP), involves considering the roles that stakeholders have in the business outside of the audit. Security audits involve identifying and rectifying issues within a company, and so any employee that may be affected by or utilise a system that is affected by the policy change or system refactoring must be considered. Employees are a good example of a stakeholder in this group, but it extends to the department heads, CEO/COO, CTO, and others in a similar position. As well as this, government bodies that enforce regulations must be considered in an audit, specifically the regulations themselves. Below is a cursory list of stakeholders that may be involved with the application of recommendations proposed by the auditing process.

- CEO/COO
- Department Heads
- Employees
- Auditors
- Government Bodies
- Suppliers/Vendors
- Investors
- Customers

(Spacey, 2016) (Faris, 2018) (Hall, 2014)

Policy changes can impact anyone in the business, ranging from employees to upper management. These policy changes often involve physical or digital security principles, specifying access to rooms like computer rooms or server rooms, as well as internet and device policies that attempt to secure the virtual network. VPNs are also included in these policy decisions, which impacts anyone connecting to the company network, securing data and communications (Verizon, 2018). These policy changes may also include business ID cards and door locking, which affects movement of employees and access privileges.

Management, including department heads, would have to identify which employees or teams that work on solving any given issue, executing an organisational process for the solution and development of the issues. Technical issues involve both frontend and backend problems. XSS (cross site scripting), code injection, access control issues and data exposure would all need to be solved by developers, whether specifically web developers, frontend and backend developers, or full stack developers. Depending on which issue, design

and testing teams would be required to extend or replace existing functionality with the policy decisions in mind.

With server-side problems, involving server or network misconfiguration, changes would involve utilising a networking team that is aware of the issues currently present and how to solve them. Database configuration issues fall under this topic also, with solutions being much more difficult to implement, depending on the scale of the database already.

Government regulations play a large part in the completion and execution of security audits, as compliance with regulation is a key part of security audits and security, with some security considerations being mandatory parts of regulations and laws. For example, the Data Protection Act 2018 and GDPR specify that information must be stored securely and have specific purposes. For this reason, government bodies must be considered based on the laws and jurisdictions that the company operates within, with regards to data laws in specific countries.

Additionally, suppliers and vendors that are not compliant with regulations or with the company security policies would have to be informed or replaced, extending the effects of the audit to these external companies. Finding new companies would require analysis of compliance and compatibility with the updated security policies. As well as this, the reputation of these companies would be considered, with low reputation companies potentially being replaced absolutely.

References

Anderson, T., 2019. *What Are the Stakeholders of a Business?.* [Online]
Available at: https://bizfluent.com/info-7752789-stakeholders-affected-interest-rates.html
[Accessed 29th December 2019].

Dube, N., 2011. *Top 5 Reasons to Conduct an Audit?.* [Online]
Available at: https://dubeconsulting.com/top-5-reasons-conduct-audit/
[Accessed 26th December 2019].

Faris, S., 2018. *Who Are the Key Stakeholders in an Organization?.* [Online]
Available at: https://bizfluent.com/info-7877597-importance-stakeholder-management.html
[Accessed 29th December 2019].

Greenlow, M., 2019. *What are the real effects of data breaches on consumer trust?.* [Online]
Available at: https://www.marketingtechnews.net/news/2019/mar/22/what-are-real-effects-data-breaches-consumer-trust/
[Accessed 26th December 2019].

Hall, H., 2014. *How to Identify and Manage Audit Stakeholders.* [Online]
Available at: https://cpahalltalk.com/audit-stakeholders/
[Accessed 29th December 2019].

Henriquez, M., 2019. *The Top 12 Data Breaches of 2019.* [Online]
Available at: https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019
[Accessed 26th December 2019].

Hinckley, D., 2015. *New Study: Data Reveals 67% of Consumers are Influenced by Online Reviews.* [Online]
Available at: https://moz.com/blog/new-data-reveals-67-of-consumers-are-influenced-by-online-reviews
[Accessed 26th December 2019].

Instructure, 2019. *Instructure Penetration Test Results: 2019.* [Online]
Available at: https://www.instructure.com/canvas/downloads/Instructure_Security_Summary_2018.pdf
[Accessed 29th December 2019].

Maxwell, L., 2014. *Four reasons why audits matter.* [Online]
Available at: https://www.helpnetsecurity.com/2014/01/02/four-reasons-why-audits-matter/
[Accessed 26th December 2019].

Reklaitis, V., 2018. *How the number of data breaches is soaring — in one chart.* [Online]
Available at: https://www.marketwatch.com/story/how-the-number-of-data-breaches-is-soaring-in-one-chart-2018-02-26
[Accessed 26th December 2019].

Spacey, J., 2016. *9 Examples of Stakeholders.* [Online]
Available at: https://simplicable.com/new/stakeholders
[Accessed 29th December 2019].

Taylor, H., 2018. *Defining and Enforcing a USB Drive Security Policy.* [Online]
Available at: https://journalofcyberpolicy.com/2018/06/03/defining-enforcing-usb-drive-security-policy/
[Accessed 26th December 2019].

Verizon, 2018. *What you need to know about business VPN.* [Online]
Available at: https://go.verizon.com/resources/what-you-need-to-know-about-business-vpn/
[Accessed 29th December 2019].