WHITE PAPER

Agiloft

Checking Your Digital Armor

The Critical Elements of Enterprise Data Security

Table of Contents

Introduction

Data security is recognized as essential to the long-term success of any business, yet it is also an area where a large proportion of organizations are deficient. This paper examines the technical, human, and corporate components of security, provides actionable recommendations, and highlights some key areas that are frequently overlooked. It concludes with a set of questions for evaluating vendor security.

Let's first define what we mean by "data security." We take it to include all the factors necessary to ensure that data is protected against loss or theft and continues to be accessible to those who are authorized to view or modify it.

This is broad definition, and many standards organizations only address data theft, not loss or breakdowns in accessibility. That may be perfectly appropriate for their area of focus, but businesses need to consider all significant threats to their data.

Attack Vectors for Data Theft

Technical Exploits

These are attacks based on vulnerabilities, such as weak ciphers, unpatched applications, and insecure networking. They are covered by the Consensus Assessment Initiative Questionnaire (CAIQ) or Cloud Controls Matrix. These questionnaires are defined and updated by a consortium of industry experts, and the answers provide clear insight into an organization's level of defense against this class of threat.

Every significant cloud vendor has completed the CAIQ or CCM. Requesting a copy and closely examining the responses is a simple, but essential, step in evaluating their security. This document provides comprehensive coverage of the basics, such as regular OS upgrades or the use of TLS in place of SSL, together with more advanced topics.

Social Engineering

Most security breaches are not the result of a brilliant hacker exploiting a software vulnerability, they are the result of social engineering such as a well-crafted phishing email that tricks an employee into divulging their email password. This allows the malicious actor to launch attacks on customers and scan for passwords leading to other systems.

The core problem is human fallibility, an area that is broader and harder to address than software vulnerabilities. The solution therefore requires multiple levels of defense.

To guard against phishing attacks, all employees should be actively trained and tested on social engineering. And the testing should include both exams and active phishing attacks by an authorized third party or internal security staff. Appropriate training materials should also be made available to customers.

To minimize the risk of a data breach if an employee is successfully phished, all email accounts and other sensitive systems should be protected by two-factor authentication. So, if an employee is tricked into divulging their password, the malicious actor should still be unable to gain access to the broader system. As an additional level of defense, emails can also be protected with digital certificates.

To minimize the damage that may be done if an employee account is compromised, the principal of "minimum necessary" access should be followed. In other words, each employee should only be able to view or edit the information necessary to do their job. As detailed here, this is a legal requirement for health information under HIPAA, and it should be applied to all sensitive company data.

Authentication

In addition to supporting two-factor authentication for access to sensitive data, authorization should be centralized though a Single Sign-On provider. This both simplifies life for the users, and provides a single point of control, so that when an employee leaves the company, access to multiple systems can be removed at once.

Access Controls

Applying the "minimum necessary" access rule to sensitive company data requires precise control over which individuals can view, edit, and delete specific information. For example, you may want to specify that Contract Managers can delete a contract if it has not been active for at least 5 years and was not negotiated with a current customer; Salespeople can edit specific

fields in a contract if a state of Negotiation and is assigned to them; and Customers can view contracts with their company.

Of course, every company has different workflows, and they evolve with business requirements and regulatory demands. So, systems must be flexible enough to both support your current requirements and adapt to changes. The alternative is that staff are given access to a lot of data that is not necessary for their job, in order that they can access the data that is relevant. Such lax permissions can worsen the severity of any security breach by orders of magnitude.

Organizational Processes

Vulnerabilities are frequently the result of staff failing to follow appropriate processes. SOC 2 has emerged as a standard for determining whether an organization has instituted and follows the information security policies and procedures necessary to safeguard customer data.

The results are audited by an accredited institution and any "findings," aka problems, are highlighted in the resulting report; but a report may still be issued if there are significant findings. So, it is not enough to ask whether an organization is SOC 2 Type 2 certified, they should also provide a copy of the report.

Decommissioning Policies

Thieves may retrieve hard drives from decommissioned equipment and scan them for confidential data. The solution is to use "encryption at rest" so that the information is unintelligible without a secret key. The active destruction of old hard drives by a shredding service provides an additional layer of protection.

Root Causes of Data Loss

There are several classes of event that can result in catastrophic data loss. But even those outside of vendor control can still be mitigated with the right hosting infrastructure. The primary causes and corresponding preventative measures are detailed below:

Disk Failure

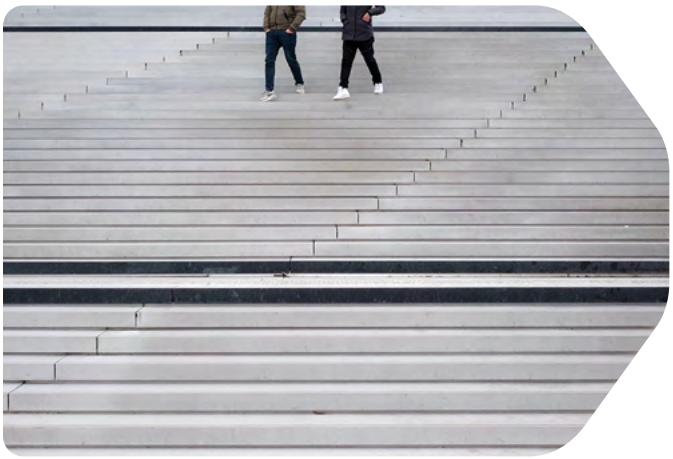
Hard drives fail and sometimes do so in rapid succession. This can be addressed by having multiple levels of redundancy, so that even if the second drives fail before the first has been replicated, no data is lost.

Acts of God

An earthquake, flood, and other natural or human-caused phenomena can destroy an entire data center. But no information is lost if the live server is replicated in real time to a distant facility.

Human Error

Administrator errors are one of the most common causes of data loss. A tired admin may click Delete Table by accident and confirm on the Warning dialog before realizing that they just deleted all their company's contracts. The solution is simply to create frequent backups, so that data can be restored with minimal loss. Daily backups are essential, and a higher frequency is highly desirable.



Ensuring High Availability

Redundancy

One key to ensuring continuous service is redundancy. Hard drives, power supplies, memory, and motherboards all fail. But when this happens, service can continue, provided there are spare servers ready to automatically pick up the load. Note the "s" at the end of "spare servers," it is important because at some point, a second server may die before the first can be replaced.

Alternate Infrastructure

Even major providers such as AWS can experience extended outages. SaaS providers can mitigate the impact on their customers, by syncing the data to another provider with alternate infrastructure for use in emergencies.

Business Continuity Planning

The business continuity plan should address the potential failure of every piece of infrastructure that could affect the SaaS service and detail how the impact would be eliminated or mitigated.

Monitoring

Monitoring is a key component of any enterprise infrastructure and is required to guard against data loss or theft, and to ensure high availability.

Hardware monitoring should alert the system administration team of hardware problems and pending issues such as the failure of one of a pair of redundant power supplies.

At a basic level, load monitoring should generate notifications if CPU usage, swap usage, disk usage, or response times exceed reasonable values. At a more advanced level, it should check for unusual load patterns since these may reflect software configuration issues.

Security monitoring should scan servers for open ports, monitor file systems for unexpected changes, and check incoming connections for attempts to reach non-standard ports.

Where appropriate, monitoring should take automated actions in addition to notifying the system administration team. For example, it might shut down all access from an IP address that tries to connect to an ssh port.

Vendor Questionnaire

Security conscious vendors will have the following information readily available; and should be willing to share it subject to an NDA. You might ask them to provide:

- Responses to the CAIQ or CCM
- The most recent SOC2 Type 2 report
- A copy of their business continuity plan
- The results of the most recent third-party application vulnerability scan
- The results of the most recent third-party network scan
- An annotated diagram of your hosting infrastructure showing the primary server(s), any replica servers, and the backup infrastructure.
- A demonstration of how they would configure permissions to address complex requirements based on your anticipated needs, and how they would change this configuration.
- A description of their monitoring infrastructure.

And to answer questions such as:

- What is the minimum number of concurrent drive failures that could cause a loss of data?
- What is the minimum number of concurrent server failures that could cause a loss of service?
- Is the data on the primary server replicated to another server?
- How far is the replica server from the primary?
- How often are the primary and replica servers backed up?
- Are all employees required to take training on defense against social engineering attacks and tested on this knowledge?
- Are employees subject to real world tests by an authorized third party or members of the security team launching phishing attacks?
- Do you share a version of your social engineering materials course work with your customers? If yes, please provide a copy.
- Are all email accounts and sensitive systems protected by two-factor authentication?

About Agiloft, Inc.

As the global leader in agile contract lifecycle management (CLM) software, Agiloft is trusted to provide significant savings in purchasing, enable more efficient legal operations, and accelerate sales cycles, all while drastically lowering compliance risk. Agiloft's adaptable no-code platform ensures rapid deployment and a fully extensible system. Using contracts as the core system of commercial record, Agiloft's CLM software leverages AI to improve contract management for legal departments, procurement, and sales operations. Visit www.agiloft.com for more.

Agiloft, Inc. | 460 Seaport Court, Suite 200 | Redwood City, CA 94063 | 650-587-8615 | 1-888-727-2209 | info@agiloft.com | www.agiloft.com