DisputeSoft
Software Dispute Experts

The Fundamentals of Data Security

Josh Siegel
Senior Manager & Forensic Examiner

Software and systems that do not adhere to best practices for data privacy and security are at risk of data breaches and security instances that may give rise to litigation.

Data privacy and security disputes often involve allegations of failure to protect consumer data, to identify a data breach and alert customers, or to implement or maintain adequate data security measures. In this article, we discuss several data security best practices that can help prevent such disputes.

Data Security Best Practices

DisputeSoft was engaged in a pre-litigation data security investigation by a financial management firm (referred to in this article as "Blue Ridge") to assess the firm's endpoint and domain name system (DNS) resolution protection software to determine whether existing protective measures were sufficient to prevent users from accessing prohibited websites and software. As part of our investigation, DisputeSoft reviewed the DNS protection software for security flaws and made a number of recommendations to the financial management firm's systems administrator.

We've drawn on industry standard best practices and our experience in the Blue Ridge matter to produce the below list of measures a company can take to assess the state of its data security practices. This list is not exhaustive, but could serve as a starting point for assessing and mitigating security vulnerabilities.

1. *Configure Firewall Protection*

A firewall is the first line of defense against attempted attacks and security breaches. It sits between the internet and a company's internal network, and serves as a gatekeeper to filter out unwanted internet traffic and only allow approved activity through. Firewalls can protect against port-specific vulnerability attacks, such as Denial of Service attacks. There are many different types of firewalls of differing degrees of sophistication, but having a firewall is necessary to block traffic from the most common threats to data security.[1]

2. *Configure Anti-Virus and/or Endpoint Security*

If the firewall is the gatekeeper for the base, then anti-virus and endpoint security software are the foot soldiers that help keep users and computers safe. Regular updates and scans with Anti-Virus and Endpoint Security software help to defend computers from viruses, secure local computer and device configurations, and isolate and remove infections if they do occur. These security softwares can help block potential threats, sometimes as they are downloaded, and prevent them from running at all.

3. *Maintain and Electronically Enforce a Written Security Policy*

A written security policy can discourage employees from misusing company resources, make them aware of the consequences, and help them consider situations they may not have anticipated. However, a strong written policy must also be enforced electronically. The risk of data loss can be minimized by classifying data according to its confidentiality level, then limiting access to only staff who need access to that data. Moreover, implementing strong group policy settings governing automatic lock screen timeouts and automatic patch and update management can help protect against unauthorized access and security vulnerabilities resulting from out-of-date software. For an extra level of protection, a company might encrypt its portable drives and devices, especially if they contain sensitive or confidential information. With a sufficient level of encryption, it is very difficult for a bad actor to recover data from a lost or stolen device.

[1] https://us.norton.com/internetsecurity-emerging-threats-what-is-firewall.html

4. *Configure Auditing and Alerting*

No one wants to experience a data breach or loss of data. However, businesses need to prepare for the possibility of a breach in advance by configuring systems to track what happened, when it occurred, and who penetrated the system. Audit logs can provide information that may be able to link activity occurring on a computer to a date, time, system, and user name. Moreover, configuring alerts to notify an administrator when users act outside of allowed or preferred security policy can help identify breaches and potentially prevent loss of data before it occurs. Such alerts may include notifications that critical systems are performing outside of thresholds, or that a log-on has occurred outside of normal business hours. When a data breach can't be stopped, a combination of audit logs and alert notifications can be used to reconstruct essential information about the breach.

5. *Implement DNS Protection and Web-Filtering*

Web-filtering options allow administrators to set lists or categories of allowed and blocked websites, while domain name system (DNS) settings on a user's computer control what websites to allow or block. Certain firewalls may include both DNS Protection and Web filtering, but they can also be implemented using separate systems. DNS protection helps ensure that a user is not able to change or circumvent settings to access prohibited websites from within a company's network. Accessing prohibited sites containing viruses can lead to data breaches or potential data loss, such as in the case of a crypto-virus. This was of particular importance in the Blue Ridge case, as the reason for the audit was an employee looking at dangerous websites from a work computer.

Conclusion

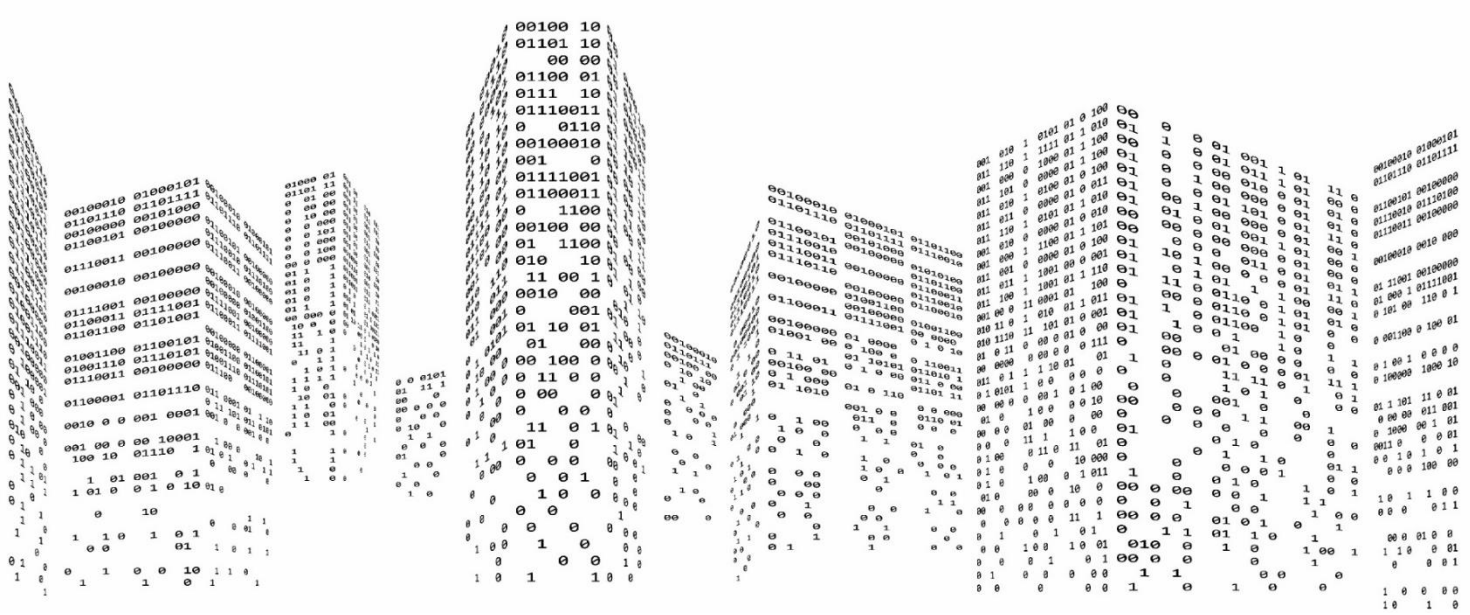
Implementing data security best practices can help companies limit the risk of data breach litigation and government investigation. Our experts work with a client's IT department in assessing data security practices, and make specific recommendations for remediating system vulnerabilities. To learn more about our data privacy and security services in the context of pre-litigation, litigation, and government investigations, view our Data Privacy, Protection, and

Security Services page. To learn more about the work we did in the "Blue Ridge" investigation, view the case write-up here: "Blue Ridge" Pre-Litigation Data Security Investigation.

Josh Siegel

Senior Manager & Forensic Examiner

Josh Siegel has substantial experience analyzing root causes of IT project failure; source code to support copyright, patent, and trade secret claims; hardware and networking; and digital forensics related to software and information technology. Josh performs functional testing, analyzes defect systems and metadata, examines source code in intellectual property disputes, acquires and analyzes data in digital forensics, and finally integrates that data into written reports and testimony.



If you are in need of a data privacy, protection, and security expert, we invite you to consider DisputeSoft.

Contact Information

Jeff Parmet, Managing Partner

301.251.6182 | jparmet@disputesoft.com

12505 Park Potomac Ave. | Suite 475 | Potomac, MD | 20854