

# Cyber-security for Business: Lessons from Equifax



Equifax, one of the three major credit reporting agencies, announced last week that hackers had potentially accessed personal data for 143 million American consumers. The wealth of names, credit card numbers, social security numbers and more constitute a gold mine for identify thieves.

In addition to a wakeup call for consumers, the hack offers important lessons in [cyber-security for business](#) owners. An increasingly complex cyber landscape requires organizations to educate themselves on emerging threats and best practices for securing data.

## Equifax Primer – What Happened?

On September 7, Equifax announced a critical breach to their system, the third in just over a year. Criminals gained access to the system in mid-May through a web site vulnerability and operated undetected until late July.

According to news sources, hackers accessed the Equifax system through a flaw in the Struts software. This widely-used program provides a framework for building web applications in Java. Through the vulnerability, cyber criminals can infect web servers with malware, enabling them to compromise data or place ransomware.

## Steps to Protect Your Personal Data

The hack means that identity thieves have potential access to personal data for one out of every two American consumers. Chances are, that means you. Consider the following steps to protect yourself, whether or not the Equifax hack impacts you directly:

- Monitor your credit – By law, you can obtain a free copy of your credit report annually from each of the three major credit bureaus: Equifax, Experian and TransUnion. Spread out your credit reports over the year.
- Check banking and credit card activity weekly.
- Implement strong passwords on all your online accounts, including shopping accounts.
- Consider placing a freeze on your credit lines – This typically involves a \$10 fee for each credit bureau. It prevents anyone (including you) from obtaining a loan or a line of credit in your name. This is strong option, but you should know how to implement it in case it becomes necessary.



As an executive, however, you take responsibility for much more than your own identity. Your customers need the assurance that you have put into effect the very best cyber-security for business and consumer data.



## Improving Cyber-Security for Business Data

Businesses safeguard a wealth of sensitive data. For your customers' protection and your business reputation, it is critical that you implement adequate security measures. To guard against hacks like the Equifax data breach, start with the following:

- Know which software frameworks you use. This could include software components you employ to create and maintain your company web site.
- Monitor security announcements and keep those components up-to-date. Often, breaches are caused when companies fail to apply fixes for months after a vulnerability is known.
- Implement multi-layer security. That way, if the public-facing layer (such as your web site) is breached, the hacker still must work through multiple additional layers to reach sensitive data.
- Monitor your web-based services for any unusual activity or access. This includes any service or tool that uses the internet, from your web site to [cloud services](#) that enable employees to work remotely.
- Implement a data encryption plan. Ensure that sensitive data is encrypted both at rest and in transit.
- Protect Guest Wi-Fi Hotspots. Additional measures are required for retailers and others who provide [secure customer Wi-Fi](#).

## Stress-Free Security

With increasingly sophisticated threats and more complex systems, implementing cyber-security for business needs can prove a daunting task. The cyber-security experts at [top managed services providers](#) offer a host of services to help your organization protect sensitive data from attack.

From secure web design and development to [network security monitoring](#) and comprehensive managed services, security-focused MSPs customize data security solutions to meet your business needs. With extensive industry experience, certified network and security experts deliver the confidence you and your customers need to prosper.