

THE BUSINESS BENEFITS OF STRONG WEBSITE SECURITY

We are now very familiar with the negative consequences of a security breach – along with the immediate fallout there is also declining revenue, damaged reputations, missing assets, regulatory fines and litigation, and decreased productivity.

Much less is said about the positive side of improving your cybersecurity.

By Georgia James

Content Writer at Siteimprove

With increased consumer expectations and ever-greater levels of digitization, businesses need to shift their thinking away from simply reducing their security risk. Now, they need to consider how a more proactive approach to cybersecurity can actually deliver real business value.

Greg Bell, US leader at KPMG Cyber, says organizations can create new business opportunities by reframing their approach to cybersecurity as a business driver. “In too many industries, information security is still seen as a technology risk to be minimized instead of a business issue to be optimized.” Once perceived as just an IT issue, businesses are now waking up to the fact that cybersecurity can provide a strong

“

In the online world of today trust is the new currency for businesses.

— Hans Nipshagen, Regional Sales Leader Web and Security, Akamai Technologies

competitive edge for businesses who get it right. Here are four ways that optimizing your website security can help you stand out from the competition and drive growth.

1 WIN NEW CUSTOMERS AND ENHANCE CUSTOMER LOYALTY

Smart businesses are now using strong cybersecurity and privacy as a selling point. A survey by Vodafone found that 89% of businesses believe strong cybersecurity will enhance customer loyalty and trust.

The same percentage thinks that security is a competitive differentiator that will help them win customers from competitors who can't offer the same assurances. "In the online world of today trust is the new currency for businesses". Hans Nipshagen, Regional

Sales Leader Web and Security, Akamai Technologies. Across every sector taking your cyber health seriously is fast becoming an essential requirement for new – and existing – customers to do business with you. When done right, cybersecurity builds trust, increases customer satisfaction, and can help you win new customers.

On the other hand, consumers have little interest in dealing with businesses that have suffered from security breaches. It's clear that consumers don't want to buy from businesses they cannot trust to protect their data – no matter how slick their product is.





“

In the online world of today trust is the new currency for businesses.

— Hans Nipshagen, Regional Sales Leader Web and Security, Akamai Technologies

Across every sector taking your cyber health seriously is fast becoming an essential requirement for new – and existing – customers to do business with you. When done right, cybersecurity builds trust, increases customer satisfaction, and can help you win new customers.

On the other hand, consumers have little interest in dealing with businesses that have suffered from security breaches. It's clear that consumers don't want to buy from businesses they cannot trust to protect their data – no matter how slick their

product is. While avoiding jeopardizing your revenue opportunities and retaining customers is reason enough to invest in good website security, an additional advantage of increased consumer confidence in your cybersecurity is being able to command a higher price point for your secure product/service.

2 PRESENT AN ALWAYS-ON WEBSITE

When a hacker uses a large network of infected systems to flood a company's servers with malicious traffic, this usually causes the targeted website to slow down, crash, or go offline.

These attacks also deny legitimate access to a website, cutting off a business's revenue stream while their site is out of action.

Organizations shouldn't overlook the profits they could miss out on if their site is targeted in this way. A single attack can bring business to a standstill and lead to weeks of disruption to business operations afterwards.



The average cost of this sort of downtime? \$5,600 per minute, according to Gartner.

According to IBM, downtime not only disturbs the flow of a business's operations, it also reduces its competitive advantage: "Today, digital business channels represent a greater market share and can drive revenue generation. Apart from revenue and productivity losses, customers do not tolerate downtime. They will quickly abandon a business and use a competitive firm to meet their needs".

In the worst-case scenario, a business may not survive the downtime and reputational damage caused by a cyber-attack.

3 REAP THE SEO BENEFITS

To protect searchers and encourage businesses to prioritize their website's security, search engines, including Google, list Hyper Text Transfer Protocol Secure (HTTPS) as one of their SEO ranking factors. HTTPS works by encrypting sensitive information such as credit card numbers, passwords, and usernames while they are

being processed on a site. Wherever possible, Google will send searchers to HTTPS-authenticated content, rather than HTTP content.

In fact, since 2018, Google Chrome will flag any website not using HTTPS as insecure.

So, having HTTPS can mean the difference between placing on page one or page two of Google. In other words, it makes bad business-sense not to do it.

On top of that, websites can be blacklisted by search engines for being malware-infected, that means lower visibility and up to a 95% drop in organic traffic that could be hard to recover from.

4 SET - AND MEET - BUSINESS PARTNER SECURITY STANDARDS

It's not just consumers that care about security and privacy safeguards. Partners, investors, and suppliers increasingly demand to see website security assessments before entering into a partnership or signing a contract. Business partnerships can be an effective growth mechanism, but they also provide an ideal environment for third-party data breaches.

With nearly half (47%) of IT professionals in a Security Magazine survey admitting they are not confident in their business partners and suppliers' security, and a security failure prompting 86% to consider terminating a contract with a supplier, there's a competitive advantage to be had for organizations with strong cybersecurity policies and processes. Having these standards in place ensures your business can apply for new and lucrative contracts and partnerships that mandate a certain degree of cybersecurity.

While cybersecurity is a huge and complicated field, gaining a better understanding of your website's vulnerabilities is a good place to start. Book a 1-1 meeting with our experts today to learn how we can help your business benefit from stronger website security. Discover more at siteimprove.com.

Siteimprove

Siteimprove is a *software as a service* solution that helps organizations fulfil their digital potential with actionable information, enabling teams to deliver a superior website experience and drive growth.

With more than 550 employees in 13 locations, Siteimprove manages more than 7,200 clients worldwide and is a member of the World Wide Web Consortium (W3C), the leading group that develops international web standards. Siteimprove is also the exclusive partner of Adobe Premier. Find out more more at siteimprove.com.



GEORGIA JAMES

Content Writer at Siteimprove

Georgia James is a UK-born, Copenhagen-based Content Writer at Siteimprove, with a particular focus on SaaS, digital accessibility, website security, and SEO.