Cyber Talk

E-COMMERCE:

GENERATE SALES WITH A WINNING SECURITY STRATEGY

Among retailers that host e-commerce sites, the massive surge in online shopping has led to new infrastructure expenditures. Because most consumers will avoid physical stores in the months ahead, many retailers with stretched budgets are investing in website re-builds and revamps.

Although your firm's exciting new e-commerce infrastructure might attract consumers, it's likely to attract hackers as well. E-commerce based businesses receive the highest volume of attacks per sector, and cyber attacks can cost organizations millions in clean-up fees.

In an age when most firms are fighting cash flow problems, poorly secured infrastructure could easily lead to further economic setbacks. To avoid this, dedicate a portion of existing funds to cyber security improvements. In addition to providing cyber protections, advanced security can help you improve client conversion rates, increase sales, and grow revenue streams. Read on to learn more.

Converting by Cultivating Consumer Trust:

More than 80% of online shoppers are wary of websites that aren't familiar.[1] Consumers want to trust your brand, but need reasons to do so. Your cyber security measures play a critical role in building customer relationships online. Where is your firm with Payment Card Industry (PCI) compliance? How about Security Socket Layer (SSL) badges? Obtaining and advertising your implementation of these methods and tactics can influence consumers' decisions.

[1] VWO, "How to Build Trust in eCommerce in 2020? [Actionable Tips]", Sachin Pandey, 04 September 2020. https://vwo.com/blog/trust-in-ecommerce/

In addition to providing cyber protections, advanced security can help you improve client conversion rates, increase sales and grow revenue streams.

Mastering PCI Compliance:

In the early 2000s, Payment Card Industry Compliance requirements were introduced as a data security standard. To be PCI compliant, organizations must:

- Maintain a firewall
- Restrict access to cardholder data
- Regularly update anti-virus software or programs
- Monitor network access

And more.

In one remarkable example of non-compliance, a hotel was found guilty of storing nearly a decade's worth of customer data, including unmasked credit card numbers, in its laundry room. PCI non-compliance and the associated reputational damage can prompt customers to take their business elsewhere.

While PCI compliance isn't legally mandated, banks often penalize non-compliant merchants. Financial penalties range from a few thousand dollars to hundreds of thousands of dollars. Non-compliant firms may also see inflated insurance premiums and lower claim payments.

On your organization's website, choose a highly visible location where you can include a statement about your organization's PCI compliance. Describe what it means to be PCI compliant and why that matters for customers. This will help build the trust that you need in order to gain and to sustain conversions.

Building your Branding with Badges:

Ninety-two percent of consumers report that they'll buy again from brands that they trust. Build trust by placing "badges" on your website, indicating that a third-party has verified your firm's credibility. A Secure Socket Layer (SSL) badge is arguably the most important badge to display, as it provides reassurance that personal information will not be stolen from a given site.

Trust badges are often under-utilized, in part due to the associated financial expenditures involved, but in the age of e-commerce, this is simply a cost of doing business.[2]

SEO, Sales, and Security as a Superpower:

Your firm's SEO strategy has the potential to facilitate a boom in sales by as much as fifty percent.[3] When sales skyrocket due to strong SEO, that's great news for everyone. However, cyber attacks can destroy your SEO optimization almost overnight, putting you on the dreaded page 3 of Google, or worse. This, in turn, can quickly lead to revenue loss.

SEO, sales, and cyber security are very much interconnected. Here's how:

Example A: The direct cyber hack.
A direct cyber hack can lead to a permanent downgrade in SEO rankings. This is because Google and other search engines only want to serve consumers high-quality websites. A site that's easily hacked isn't considered a quality site. It may even become blacklisted. Long-term, Google's SEO penalties can lead to significant sales slumps.

Example B: Battling the bots.
Roughly 20% of cyber bots on the internet scrape content, steal data or otherwise behave in malicious ways.[4] Bot-based attacks may prevent Google's website crawlers from accurately categorizing the pages on your site. While a single attack by a cyber bot won't spoil your SEO rankings, repeat cyber bot attacks can. They throttle your website traffic and as a result, your server may cease serving pages, turning up 404 or 503 errors. When error codes occur frequently, Google downgrades sites. As in the previous scenario, a site may even become blacklisted.

When building your SEO strategy, be sure to integrate security. Advanced cyber security protections can help you prevent website ranking downgrades, enabling you to maintain or increase your sales.

[2] Entrepreneur, "How to Make Your E-commerce Site More Trustworthy," Syed Balkhi, 4 October 2019 https://www.entrepreneur.com/article/339286

[3] Optinmonster, "The Ultimate eCommerce Optimization Guide: 13 Steps to Instantly Boost Revenue," Sharon Hurley Hall, 3 January 2020 https://optinmonster.com/ecommerce-optimization-guide/

[4] ZDNet, "Bad Bots Now Make up 20% of Web Traffic," Charlie Osborne, 17 April 2019 https://www.zdnet.com/article/bad-bots-focus-on-financial-targets-make-up-20-percent-of-web-traffic/#:~:text=Bots%2C%20in%20general%2C%20are%20estimated,generated%20by%20bad%20bots%20alone

Revenue Growth Opportunities: A Security-First Approach

A large swath of e-commerce organizations have recently transferred their IT systems to the cloud. "Many customers are scaling beyond their wildest projections," says Carrie Tharp, who oversees consumer strategy at Google Cloud.[5]

The cloud can offer non-linear revenue growth opportunities, enabling firms to quickly support new initiatives and respond to market demands. Projects can move forwards in a matter of days, rather than months. This can yield new earning potential and broaden a company's customer base.

Many customers are scaling beyond their wildest projections," says Carrie Tharp, who oversees consumer strategy at Google Cloud.[6]

The ability to easily grow new revenue streams via cloud computing can prove hugely profitable, provided that your cloud does not suffer any data breaches. And cloud-based breaches are common. Take a security-first approach and don't lose out on growth opportunities due to breaches. Optimize your business operations with automated and unified cyber security solutions. Security can help you maximize your potential, limit your losses, and make you more profitable.

A Case Study

The e-commerce mobile shopping and payment platform known as Omnyway is PCI certified, but they wanted to enhance security and compliance measures. The company's customers consist of several Fortune 500 retailers and other large enterprises.

"As our platform channel continued to grow with more applications being developed, our environment was becoming very complex. It was becoming difficult to visualize our VPC peering, security groups, and workflows to verify our environment was secure. We also needed a secure yet flexible way to accelerate our DevOps by providing developers with easy remote access while making sure ports remained closed when not in use," among other things, says Robert Berger, CTO and SVP Engineering.

[5] PYMNTS, "Online Sellers Rely on Cloud to Handle Digital Surge," 24 August 2020 https://www.pymnts.com/news/ecommerce/2020/online-sellers-rely-on-cloud-to-handle-digital-surge/

[6] Ibid

To gain granular visibility, misconfiguration identification, customized policies and access control - all of which contribute to business success - Omnyway choses Check Point.

Learn more about their decision here.

In Conclusion:

Cyber security is now a cornerstone of modern e-commerce based businesses. Reassess how you can leverage it to not only protect your business, but to build a bigger and better business. Strong cyber security increases consumer trust and boosts sales. In addition, it helps to ensure that your SEO strategy will not falter and supports you in maintaining marketshare and profitability from new revenue streams.

Carefully considered security investments and implementation are a huge win all around. Customers gain the confidence that they need to make purchases, and firms meet calculated sales goals and revenue targets. Take your cyber security to the next level today.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com