Prioritize Cybersecurity to Protect Your Business Before It Is Too Late



December 16, 2020 6 min read

Opinions expressed by *Entrepreneur* contributors are their own.

In the world of business, revenue is king — and understandably so. A business can only grow if it's generating revenue, and a business operating without a clear path to revenue isn't long for this world.

That said, obsessing over short term profit — and only profit — can cause entrepreneurs to ignore other essential parts of their businesses. If entrepreneurs only focus on making as much money as possible as fast as possible, they will likely neglect security and the stickiness that comes with trust — and pay for it in the long run.

What Happens When Security is an Afterthought

Cybersecurity needs to be at the forefront of every business, especially large enterprises, but it too often isn't. Some entrepreneurs think emphasizing security can hold back innovation. Others believe it costs too much, in terms of both manpower and money. There are also those who simply haven't prioritized it.

The unfortunate fact is that if you don't give your company's data security attention, the bad guys will. Just look at a few recent incidents that arose because companies, in retrospect, considered security as an afterthought.

Zoom's Security Claims

As reported in TechCrunch, Zoom recently reached a settlement with the FTC regarding the company's claims about using end-to-end encryption. Apparently, the company wasn't. The FTC called the company out and forced Zoom to change its practices to no longer misrepresent its security measures. In Zoom's case, the promised security was an afterthought.

Twitter Hacked Through Slack

Back in July, Twitter saw several big accounts hacked to promote a bitcoin scam. According to Mashable, the hacker gained access to Twitter's systems via unprotected credentials on the company's Slack account. In this instance, security on Twitter's Slack account was an afterthought.

Microsoft

In April, Microsoft Teams experienced a vulnerability that could have allowed attackers to use a malicious GIF image to steal data from that company's accounts. Threatpost says

researchers at CyberArk identified the threat, and Microsoft subsequently patched it. No data was stolen, but it could have been, all because Microsoft viewed Teams security as an afterthought.

Since these companies are all household names, it is clear that they survived their breaches. However, keep in mind that these are large, multi-billion-dollar companies that have run the gauntlet to become too big to fail. What does a data breach mean to a small business, one just entering this gauntlet?

Research shows that 60% of small businesses have to close their doors within 6 months of a cyber attack. So rather than focusing on how these businesses bounced back, smaller businesses should take these incidents as an important warning sign – they likely won't be so lucky to survive such an attack, and as such, should learn from the mistakes of these larger companies and make sure that security is a priority from the start.

Related: Cybersecurity Practices That Protect Your Small Business

How to Do Security the Right Way

It's not difficult to do the right thing when it comes to security. It's a simple matter of taking security seriously – and knowing that malicious actors are deliberate, persistent, and patient in their actions. They are deliberately planning events that can exploit holes in your security. They are persistent in pursuing different avenues of attack, and they are patient and capable of waiting for the right opportunity to pounce.

In return, your cybersecurity efforts should also be deliberate, persistent, and patient. Deliberate in your efforts to protect your data and systems, persistently

improving your security, and patient in building a long-term secure environment.

You can differentiate your company by paying attention to these points and stressing security throughout your organization and software development lifecycle. As important as enterprise security is, it comes at a cost. All the malicious actors out there will want to test your security assertions. Of course, they'd also be testing you if you didn't strengthen your security. Better to be ready for them than unprepared.

Related: Cybersecurity Implementation And Future Strategies For Enterprises

Cost vs. Security

Some executives question the cost of enterprise security. It's fair to evaluate the cost versus benefit of any business endeavor, but in the case of cybersecurity, you'll find that the investment is necessary. Great enterprise security might involve more work and incur more upfront costs, but that's nothing compared to the cost of ignoring security and then potentially falling victim to a breach, ransomware attack, or releasing a vulnerable product.

All you have to do is compare the cost of cyberattacks to spending on cybersecurity. Gartner forecasts that global spending on information security this year will be almost $124 billion. You might think this sounds like a lot, but once you realize that the global cost of cyberattacks will reach $6 trillion a year by the end of 2021, according to Cybersecurity Ventures, it doesn't seem so drastic. The damage of cyberattacks is still outweighing the cost of cybersecurity and will continue to do so.

The Importance of Transparency

Despite the benefits of strengthening your company's cybersecurity, the cost of this security can be insurmountable unless you adopt a practice of transparency. By embracing transparency, you can help make cybersecurity more affordable and effective for you and others.

Transparency in security means opening up your code, hiring the best security experts to test your product, and opening up your results. It's also important to support bug bounty hunting by building it into your security QA processes – the more eyes on the process, the better. Internal transparency is also key. Building a culture of unit testing and security-based CI/CD is an important way to make sure your team is pulling together to build better and more secure products. The important win here is that these processes create better and more performant products that just happen to be more secure.

Related: 6 Cybersecurity Must-Haves For Your Business

Characteristics of Security Done Right

What does it look like when security is done right? There are key characteristics:

- In the case of products that make cryptographic promises, using an open protocol/source code for enhanced transparency is mandatory.
- Security is built into, not bolted onto, your systems and processes. If you are a development organization without unit testing, then you are not committed to security.
- Zero trust security principles are embraced and extended

beyond end users. Don’t automatically “un-trust” only your end-users. This philosophy should be extended inside or outside your perimeters – including your security team and your service providers!

If your company can embrace these approaches, you will reduce your risk factors and better protect your company’s – and your customers’ – data. It may not always be an easy path in the short term, but in the long run, you will have more loyal customers and avoid the hyper-expensive process of scrambling to patch and respond.

https://www.entrepreneur.com/article/360899