


FORBES > INNOVATION

How Prioritizing Cybersecurity Can Give Your Company A Competitive Edge

 **Justin Rende** Former Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

 Aug 14, 2024, 06:45am EDT

 *Justin Rende is the founder & CEO of Rhymetec, a cybersecurity firm providing cybersecurity, compliance and data privacy to SaaS companies.*



GETTY

Cybersecurity has had an interesting trajectory so far. It developed into a **unique discipline** during the 1960s and '70s, gaining widespread public attention in the late 1980s after several incidents highlighted the risks of inadequate security measures. Now, however, it's no longer just about safeguarding data. Cybersecurity has become a strategic component that can drive business growth. Companies with robust cybersecurity measures can benefit from multiple advantages while those that don't can fall victim to bad actors—quickly and stealthily. Here are some primary reasons for companies to prioritize cybersecurity.

Enhancing Trust And Referrals




Customer confidence and revenue are inescapably intertwined. **Research by Gartner** shows that 81% of customers will avoid buying from companies they don't trust. What's more, 89% will walk away from a brand that doesn't live up to their expectations in this regard. This makes managing trust a critical component of customer retention.

A robust compliance record is crucial for enhancing a company's cybersecurity posture, with SOC 2 and ISO 27001 heading the list. These frameworks require rigorous security assessments, so achieving them provides credibility. This can lead to increased referrals, as satisfied clients and partners are more likely to recommend a trusted company.

Driving Competitive Differentiation

A robust cybersecurity program can also significantly differentiate a company in a crowded marketplace. Firms with strong security measures are more likely to attract customers who prioritize data protection. Because **94% of consumers won't buy** from a company they don't trust to protect their data, businesses can set themselves apart by demonstrating a commitment to cybersecurity.

MORE FOR YOU

- [TikTok Ban: Trump Suggests He'll Delay Ban—Here's Everything We Know](#) 
- [FBI Warns iPhone, Android, Windows Users—Do Not Install These Apps](#) 
- [New Hacking Disaster Warning For Gmail, Outlook, Apple Mail Users](#) 

Attracting high-quality talent and partners is another way for companies to differentiate themselves. Prospective employees increasingly consider cybersecurity practices when choosing employers because they prefer working in secure environments. Similarly, potential partners and investors are more likely to engage with companies that have a proven track record of safeguarding information, so showcasing a strong security posture sends the right message.

Protecting Company Reputation

Data breaches can have devastating effects on a company's reputation. They lead to financial loss and erode trust among customers and partners. Data breaches reached an average cost of **\$4.45 million** in 2023, signaling a 15% rise over the preceding three years. According to the **Institute of Data**, such breaches often result in damaged reputations, and companies face a long road to regain trust and restore their public image.

Minimizing Financial Risks

Cyberattacks such as phishing and ransomware pose significant financial threats. The global cost of cybercrime is predicted to reach **\$10.5 trillion annually by 2025**, highlighting the urgent need for businesses to assess their vulnerabilities.

Conducting A Risk Assessment

A comprehensive risk assessment should be your first step in addressing cyber threats. This involves examining internal and external environments such as governance structures and market trends. To achieve this, you need to:

- Determine your risk level by maintaining an asset inventory, recognizing potential threats and assessing vulnerabilities.
- Engage stakeholders to identify risk scenarios.
- Analyze risks by assigning numerical values to their likelihood and impact, classifying them as high, medium or low.
- Prioritize risks for treatment, developing a detailed plan that outlines actions to mitigate identified risks, including responsibilities and expected outcomes.
- Evaluate the potential impact of cyberattacks on your business.

This systematic approach ensures effective identification, analysis and mitigation of potential cybersecurity threats.

Implementing An Incident Response Plan

Having an incident response plan in place is invaluable for managing cybersecurity threats. It allows a company to respond quickly and effectively to cyberattacks, minimizing downtime and financial loss. Companies with incident response teams can save up to **\$2 million per breach**.


Your incident response plan should include the following key components: preparation, detection and analysis, containment, eradication, recovery and post-incident activity. Our own plan follows these steps meticulously. We prepare by establishing clear roles and communication channels. During detection and analysis, we identify the scope and impact of the incident. Containment strategies are implemented to limit damage, followed by eradicating the threat. Recovery involves restoring systems to regular operation, and post-incident activities include a detailed review to improve future responses.

Keeping Up With Developments

Cybersecurity is pivotal in driving business growth. As cybercrime grows and threats become increasingly sophisticated, companies that invest in building a sturdy cybersecurity program will have a valuable asset to help them capitalize on new opportunities. Keeping up might seem daunting because threats change daily, but having a strategy in place that monitors new developments and actively promotes action is critical for company success.

Forbes Technology Council is an invitation-only community for world-class CIOs, CTOs and technology executives. *Do I qualify?*

Follow me on [Twitter](#) or [LinkedIn](#). Check out my [website](#).

 **Justin Rende**

Justin Rende is the founder & CEO of [Rhymetec](#), a cybersecurity firm providing cybersecurity, compliance and data privacy to SaaS companies.

Editorial Standards

Forbes Accolades

MORE FROM FORBES

Jan 17, 2025, 08:15am EST

How To Choose The Best BPA Vendor For Your...

Jan 17, 2025, 07:30am EST

2025 Manufacturing Predictions: The Rise Of...

Jan 17, 2025, 07:15am EST

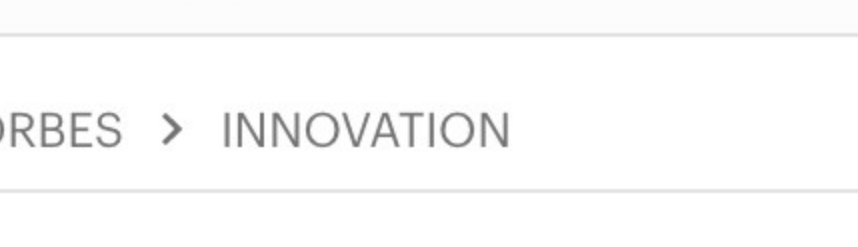

The Future Of AI Is Completely Personal

Jan 17, 2025, 07:00am EST

A Marathon Of Innovation: 4 AI Technologies To...

ADVERTISEMENT

Just starting your SEO iourney?

[Learn More](#)

FORBES > INNOVATION

The AI Edge: Transforming Business Growth In The Digital Era

 **Chris "Jay" Hawkinson** Forbes Councils Member
Forbes Technology Council COUNCIL POST | Membership (Fee-Based)

 Jan 17, 2025, 10:02am EST

 *Chris "Jay" Hawkinson is the Senior Director of Data & Analytics at Lamb Weston.*



ADVERTISEMENT



Give blood, give hope.

Help us get to **450 new donors** a day to fuel **Canada's Lifeline**