WHY OVERLOOKING NETWORK SECURITY SOLUTIONS RISKS YOUR BUSINESS

By Janine Griffiths | August, 22, 2021 | IT Insights

Facebook 0

Twitter 0

LinkedIn 0

A security guard asleep on watch would be fired. But what about network security that allows cybercriminals through the door without a fight? These days, it's accepted as the price of doing business. Dell, which polled IT decision-makers nationwide, found out that only 18% of businesses incorporate security planning into their digital transformation strategy. But enterprises that choose to overlook network security solutions will quickly find they made a grave mistake.

1.) HACKS ARE ON THE RISE

Data breaches are on the rise with601 reported cases thus far in 2016 (we can almost guarantee there will be more by the time you read this). That we know of, more than 13 million records have been compromised and there are presumably millions more that are yet to be recognized as compromised.

Organizations of all sizes across industries are being targeted. Healthcare providers, social media platforms, government organizations, and media companies have been breached this year and the spectrum of victims will diversify further by year's end.

The lesson that every business should acknowledge is that no one is immune to being singled out by cybercriminals. Robust network security solutions are not just the priority of Fortune 500s and government agencies. Your data is often worth the effort cybercriminals put into an attack. Social security numbers can go for $30, dates of birth for $11, and health insurance credentials can go for $20 on the black market. Getting data in bulk makes it lucrative.

Plus, chances are good that even if the data isn't the target, a breach through your network can provide them with a lead to another.

2.) CLOUD SOLUTIONS AND 3RD PARTY VENDORS CREATE VULNERABILITY

How many facets of your business are run by cloud providers or 3rd party vendors? We increasingly outsource everything but our core deliverability, relying on platforms and services provided by the experts to give our companies an edge. That model is practical, but a trade-off comes to network security.

Remember the Target data breach a few years back? The retailer lost customer names, account data, credit/debit numbers, expiration dates, CVV security codes, and PINs in a data breach. And the culprits compromised Target's otherwise strong network security solutions for their point-of-sale system, by hacking a third party vendor that obtained them access to Target's maintenance and utility network and easily connected them to the main network. In the end, it was the vulnerable network security of Target's vendor that precipitated the breach worth billions of dollars.

And cloud applications are not getting off lightly. Though most hacks occur in data on-premises situations, there are examples of cloud hacks. The iCloud hacks happened through a security issue with the iCloud API, essentially granting unlimited tries for hackers to guess passwords. Given time, any brute force attack prevails.

With more applications, platforms, and vendors being entangled within daily operations, the selection of high quality partners is all the more important. The strength of their network security solutions becomes an extension of your own, making it all the important to have strong internal resources.

3.) CYBERSECURITY TACTICS ARE EVER EVOLVING

Even businesses putting emphasis on network security in the past can still be vulnerable. More employees are accessing secure networks with unsecure devices. Zero day vulnerabilities lingering in untested network security solutions are ticking times bombs for cybercriminals to capitalize on. Plenty of network security vulnerabilities are lurking just out of sight.

On the plus side, cybersecurity tools are expanding to win the war against cybercriminals.Machine learning tools are being directed at network security solutions, detecting common anomalies and preventing enterprises from being breached. Microsoft EMET (Enhanced Mitigation Emergency Toolkit) helps to spread awareness to internal workers about cybersecurity threats. Plenty of tools exist that network security solutions only a few years old would lack. Businesses that fail to integrate the latest tools will provide an ever-expanding window for hackers to utilize.

BRINGING NETWORK SECURITY SOLUTIONS UP TO SPEED

The rise of hacks, the integration of 3rd party vendors into enterprises, and the evolution of cybersecurity tactics require an expert's touch to prevent cybersecurity threats. The talent gap makes finding exceptional cybersecurity talent to face those threats difficult. That's why it's important to use all available resources to fill that essential position.

EdgeLink can provide that cybersecurity connection. Our team of IT staffing professionals has extensive experience with a wide range of IT specialties across industries and can find networking security professionals that fit your needs. To find the full scope of what we can do, check out our Services page and get one step closer to providing critical protection to your business.

« Job Interview Tips: How to Prove You're a Purple Squirrel
Lowering the Average Cost Per Hire of IT Talent»

OUR STORY | SEARCH TECH JOBS | STAFFING REQUEST FORM | BLOG | CONTACT US

CONTACT:

PORTLAND: 503.246.3989
DENVER: 303.953.4374
SALT LAKE CITY: 801.937.9646

OUR REVIEWS
★★★★★
4.76 (1747 reviews)

CLEARLYRATED STAR RATINGS:

EdgeLink, LLC

CLIENT RATING	TALENT RATING
★★★★★ 4.6	★★★★★ 4.8
BASED ON **43** VERIFIED CLIENT RATINGS	BASED ON **118** VERIFIED TALENT RATINGS

SEE ALL OUR RATINGS AND TESTIMONIALS > clearlyrated

BACK TO TOP