Growth requires security

Cyber Weakness Hurts Innovation

Deflecting cyberattacks is certainly a pressing concern, but a more troubling outcome of weak cybersecurity is its impact on company growth and innovation.

In a recent study by Cisco, a stunning 71 percent of executives said concerns over cybersecurity had impeded innovation at their companies. Among respondents, 39 percent said they had halted mission-critical initiatives due to cybersecurity issues. These responses highlight how cybersecurity weakness impedes the ability of firms to innovate at precisely the time they need to do so to compete.

Digitisation, disruption, and exponential change have become the new normal of an intensely competitive business environment. Nimble businesses can establish a clear lead over the competition if they can innovate, move quickly, and reward experimentation.

A Breach Impacts More Than the Bottom Line
Failing to secure your network can have far-reaching consequences, including: downtime, equipment damage and replacement, incident response, forensic investigation, internal audits and communications.

A loss of customer confidence can permanently damage a previously strong revenue stream. Losing your customers' data may result in legal action, fines, increased regulation and remediation costs. Yet the damage does not stop there. For example, if a retailer suffers a data breach, customers may not feel comfortable sharing personal information anymore.

Your business can gain a decisive advantage by harnessing:

- Established technologies such the web, mobile, cloud, enterprise resource management, and customer relationship management

- Fast developing technologies like artificial intelligence and data analytics

These technologies help businesses better connect with their customers, reach new markets, and enhance worker productivity, while also boosting revenues and cutting costs. Cybersecurity concerns can hinder the pursuit of some digital business models and innovations.

Damned if you do and damned if you don't
Many business people have a bad choice. A risk of getting it wrong or a risk of getting left behind. They feel they must continue to press forward or

They feel they must continue to press forward or risk being overtaken by digital disruptors and other agile competitors. In our survey, 73 percent of respondents admitted they often embraced new technologies and business processes, despite the cybersecurity risk.

Sub-par cybersecurity leaves businesses in the worst possible competitive position: not innovating fast enough to compete, yet not safe enough from cyber attack, despite delaying digital innovations.

How would a security breach or a ransomware attack affect your business?

What is the potential financial impact of a network outage due to a security breach, or loss of access to data and systems due to a ransomware attack?

– Could a security breach or ransomware attack disrupt your supply chain?
– What would happen if an attack caused your website to go down?
– Does your company rely on e-commerce features on its website?
– How long could the site be down before your business lost money?
– Is your company insured against cyber attacks, or against the misuse of your customers' data? Is this insurance adequate?
– Does your company have backup and recovery capabilities to restore information, if necessary, after a security breach or loss of data due to a ransomware attack?