The Cyber Shield: Safeguard Your Business with Best Practices

Submitted by mtriquell@hote… on Mon, 30/09/2024 - 09:12

*The Knox Corps CEO, **Scott Patterson**, explores how travel professionals can protect their businesses by following cybersecurity best practices.*

I'm Scott Patterson, CEO of The Knox Corps. I'm also an accomplished information security executive, with over two decades of experience strategising and developing enterprise security programs for highly regulated organisations in sectors such as healthcare, financial services, and the United States Air Force. Additionally, I serve as the Sector Chief of the FBI's Communications sector and as a Governor of Homeland Security. Given my background, I am deeply immersed in the world of cybersecurity.

As part of **Cybersecurity Awareness Month**, I'd like to take the opportunity to share some of my knowledge to help you and your business stay safe.

Cybercrime is a serious threat. There are organisations that, if attacked today, might not survive tomorrow. It's a daunting reality. In the event of a breach, not only could a business face closure, but sensitive information — including financial and confidential customer details — could be compromised. Understanding how to strengthen security measures and implement an effective disaster recovery plan can be the key to either withstanding an attack or falling victim to it.

Compliance is King

Is the travel industry a prime target for cybercrime?

Yes, absolutely. In addition to the reasons outlined, there are **many access points to this sector**. Here's a simple analogy: the more doors that you have to your house, the more susceptible you are to your home being compromised. If you have one door, you only have one to secure; if you have two or three, you need to be much more vigilant.

This is the case in the travel industry – between email communications, telephone calls, third parties, partnerships, websites, and even payments, several areas could become compromised. This is where compliance comes into play.

Dual Compliance

The travel industry falls under what I'd refer to as 'dual compliance', where players must comply with multiple regulatory bodies.

The first is the **Payment Card Industry**, or PCI, which has its own set of standards around securing the financial transactions surrounding the credit card and the credit card holder. PCI is only concerned with what was mentioned above since hotels must get paid, and the number one form of payment is via e-commerce, either web or in person. There is a separate council that governs and enforces PCI, and the cost of a breach could be substantial.

On the other side, we have **ISO compliance**, which handles breaches related to all personally identifiable information (first and last names, addresses, the names of family members, health information, bank account information, emergency contact information, email addresses, and so forth). As you can imagine, balancing the different areas of compliance can be complex, and this is where I recommend a **risk assessment**.

A proper risk assessment covers technical and non-technical risks, providing a global perspective of dual compliance, where risks are aligned under each regulatory body and a mitigation plan is in place to remediate. In the end, one must have proof of such by way of what's called a Report on Compliance (ROC).

Enhanced Security, Greater Success

Understanding the resources available to you is crucial. I get it — not every company has thousands of dollars, euros, or pounds to hire in-house security specialists. However, I can't emphasise enough the **importance of proper compliance and risk assessment**.

Let me explain why.

Without due diligence, your company may not survive. Countless businesses have gone under due to a lack of preparedness. We are living in an age of technological advancement, and with that comes an increased risk of cybercrime. Staying up-to-date and well-protected is essential for your company's survival, as well as for the security of your customers and partners.

Customers and partners value security. Think about it — when choosing between two companies, what's the differentiator? Today's partners and consumers are becoming increasingly savvy and concerned about their online safety. On the partnership side, every brand wants to protect its assets, whether financial data, customer information, or a hard-earned reputation.

Demonstrating a **commitment to security** can help you win their business by showing that you share their concerns.

So, How Can You Implement Cybersecurity Solutions Without a Dedicated Team?

This is where companies like **The Knox Corps** come in. We provide risk management, ethical hacking, forensics, vulnerability assessments, IT security, and advisory services to help you become cyber-compliant. That way, you can focus on delivering great solutions to your customers.

I'd like to extend my gratitude to HBX Group for giving me and The Knox Corps the opportunity to address this important issue. Alongside Christo and Paula, we are committed to raising awareness about cybersecurity—outreach is essential.

There's one final thought I'd leave you with during this Cybersecurity Awareness Month: it's to **remain curious yet cautious** about the digital world's constantly evolving nature (consider the rise of artificial intelligence, for example). With that evolution, it's vital to arm yourself with the knowledge needed to protect your business and yourself before you venture toward bolt-on solutions, such as artificial intelligence. Keeping up with trends while performing trend analysis is paramount to the success of your business. So, before focusing on trends, focus on the foundation first.

Scott Patterson is an entrepreneur, professor, professional speaker, and Advisory Chief Security Officer. He possesses over two decades in organisational leadership roles, with proven experience in strategising and developing enterprise security programmes for highly regulated organisations in Healthcare, Financial Services, Education Insurance, and the Armed Forces.

Thumb image