Compliance vs security ...what's the difference?

While compliance and security are often related, compliance is focused on meeting specific requirements and standards, while security is focused on protecting against threats and vulnerabilities.



Compliance

An organization may be compliant with certain regulations but still have vulnerabilities in its security systems.



Security

On the other hand, an organization may have robust security measures in place, but still fail to meet certain compliance requirements.

Contact centers at risk Organizations need to prioritize both compliance and security to protect

their people, customers, assets and operations effectively.

Humans account for

Did you

know?

82% of data breaches

89% of US contact centers

will continue to have home-working agents 83% of organizations have had

more than one breach

\$4.4 Million

> is the average cost of a data breach



Cyber-attacks

Contact centers may be targeted by cybercriminals seeking to gain access to sensitive customer data or disrupt operations. This can include attacks such as ransomware, phishing scams and other forms of malware.



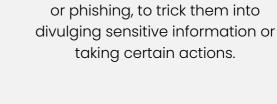
Contact centers handle a large amount

of sensitive customer data, making them vulnerable to data breaches. These breaches can occur when unauthorized individuals gain access to customer data and can result in the loss or theft of this data.

have robust security measures in place and to educate employees on identifying and preventing them.

To protect against these threats, it's vital to







Fraud Contact centers may be targeted by

individuals seeking to commit fraud, such as by making false insurance claims or attempting to obtain confidential information through deceit.

How can you secure my customer contact center?

There are a number of steps you can take to secure your customer contact center:

attackers to steal: Remove and prevent sensitive

data from entering, or being stored within, your organization. Eckoh's Security Suite enables customer card payments in multiple channels.

Leave nothing for

Implement robust network security: This can include measures such

as firewalls, intrusion prevention systems and network segmentation to protect against cyber-attacks.

password management: Ensuring that your employees use strong passwords and

that these passwords are managed securely can help prevent unauthorized access to customer data.

Implement strong

passwords and

Implement data security This can include encrypting

sensitive data, using secure

servers and storage systems, and implementing access controls to ensure that only authorized personnel can access customer data.

5. Create a security: Educating your employees on best information security

practices, such as identifying and preventing phishing attacks, can help protect your contact center from cyber threats.

Create a culture of

6 measures for remote workers:

If your contact center

employees work remotely, make sure to implement security measures such as virtual private networks (VPNs) and secure remote access systems to protect against cyber threats.

• relevant regulations and standards: Make sure to comply with

Become compliant with

any relevant regulations and standards, such as the California Consumer Privacy Act (CCPA) and the Payment Card Industry Data Security Standard (PCI DSS), to ensure that your ontact center is secure

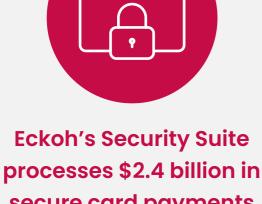
response and disaster recovery plans: Having a plan in place for

Implement incident

responding to and recovering from cyber incidents or natural disasters can help protect your contact center and minimize disruption to operations.

Why work with us?

Eckoh



secure card payments each year



PCI DSS level 1 compliant since 2010 - the longest in the industry





Secure all channels in your contact center with technology that wraps around your existing tech stack