INTERNAL THREATS & SCARES

DON'T BE HAUNTED BY SPOOKY INSIDER THREATS THIS HALLOWEEN, LEARN HOW TO ELIMINATE ANY SKELETONS IN YOUR CONTACT CENTRE

HATEFUL HACKER

Threats are becoming more complex as hackers hone their skills and identify vulnerabilities. They are capable of writing their own attack programs and often building their own platforms in order to target organisations. If malware gets installed directly in your payment portal, the hacker has access to countless payment card data in a matter of seconds.

MOTIVES

- **FINANCIAL GAIN**
- **DISRUPTION**
- **ESPIONAGE**

START WITH... IMPLEMENTING AN INCIDENT RESPONSE PLAN

18%

OF LAST YEAR'S DATA BREACHES WERE CAUSED BY INSIDERS

START WITH... REVIEWING WHO HAS ACCESS TO DATA AND REMOVING COMPENSATING CONTROLS

INSIDIOUS INSIDER

Insider threats continue to present a great risk for organisations because they can be extremely hard to prevent, detect, and contain. With the contact centre industry's high employee turnover rates and hybrid workforce, sensitive company data can easily be mismanaged, stolen, or even sold by malicious employees within your organisation.

NEEDLESS NEGLIGENCE

Many employees would never consciously harm the organisation. However, they can easily put the company at risk by neglecting basic data security practices. Leaving laptops open and unattended, joining an unsafe public WiFi network, or failing to recognise a phishing email can quickly lead to the misuse of valuable data.

THE AVERAGE COST OF AN INSIDER-RELATED INCIDENT IS

$8.76M

START WITH... CONSISTENT TRAINING OF EMPLOYEES

39%

OF BREACHES INVOLVED MISUSE OF DATA BY AUTHORISED USERS

START WITH... STRICTLY CONTROLLING PHYSICAL ACCESS

OVERLOOKED OUTSIDER

While your organisation may be diligent when it comes to employee security practices, don't overlook potential threats from third-party vendors, contractors, or even the maintenance staff. Your partners or your office staff could easily take advantage of the data they have access to within your organisation, whether that is online or offline

'DO NOTHING' DEMON

Although it has been 18 years since the introduction of the PCI Data Security Standards, many organisations are struggling to keep up with the evolving requirements and still use compensating controls that are no longer sufficient. Not only does that make these organisations a prime target, but banks and merchants can refuse to work with non-compliant companies entirely.

73 DAYS

IS THE AVERAGE TIME IT TAKES TO FULLY CONTAIN AN INCIDENT

START WITH... REVIEWING THE UPDATED PCI DSS v4.0

? WHAT NEXT? DESCOPE.

Face these threats head-on by **descoping** your contact centre. In addition to trying to keep hackers and threats out, businesses should focus on reducing or removing the sensitive data they handle, ensuring there is not any data to be stolen in the first place. At PCI Pal, we support businesses in minimising risk by ensuring valuable data is not managed, processed, or stored within an organisation's contact centre environment.

Source: Data Breach Investigations Report by Verizon
View more PCI Pal resources at www.pcipal.com/knowledge-centre/