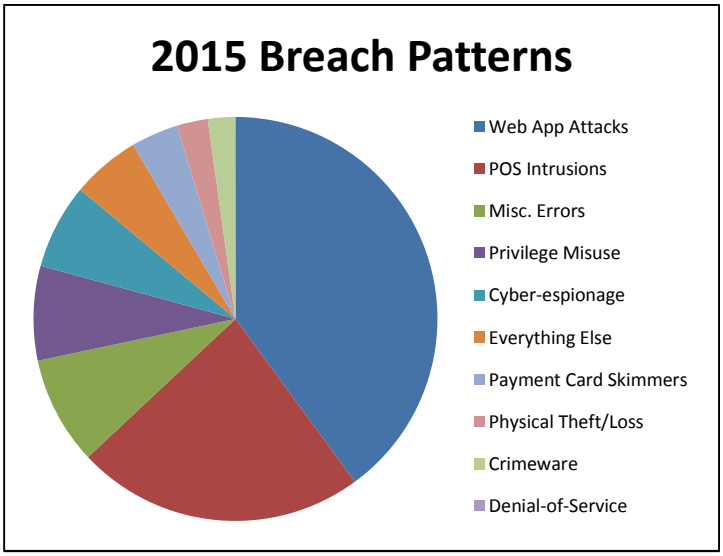
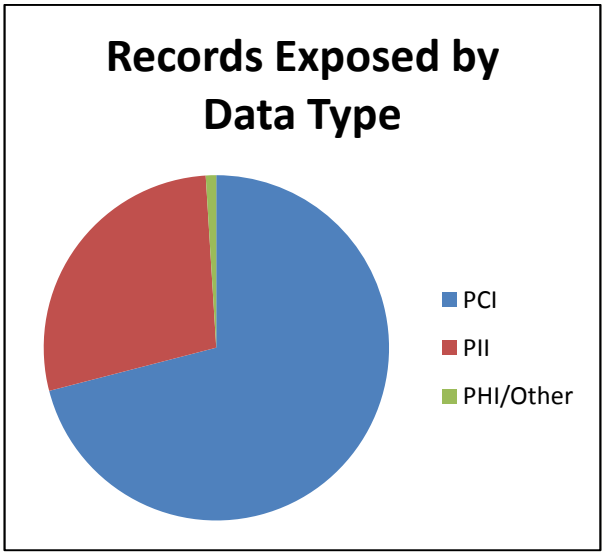
Cyber Liability Can't Be Outsourced

Whether small, midsize or large, businesses across virtually all industries are vulnerable to cyber incidents and data breaches. The overwhelming majority of cyber-attacks are motivated by financial gain, which increases the exposure of *all organizations* holding data that cyber criminals can sell, and the resulting liability for cyber risks cannot be outsourced.



Source: Verizon Enterprise Solutions, *2016 Data Breach Investigations Report*



Source: NetDiligence, *2015 Cyber Claims Study*

Merchants are especially at risk for theft of information such as payment card numbers. Exposure of payment card information is a serious problem on multiple fronts, not least being third-party liability. First-party expenses arising from a breach are larger and more complicated than many businesses realize. Forensic investigations, breach notification, legal services and other expenses can mount quickly even following a relatively small cyber event.

CRC PERFORMANCE IS THE DIFFERENCE™

Swett & Crawford

Of particular concern are costs relating to payment card information security. Merchants accepting payment cards are responsible for complying with the Payment Card Industry Data Security Standard (PCI DSS) and can face fines and assessments, as well as requirements to conduct forensic investigations by a qualified PCI Forensic Investigator.

Even when using a third-party vendor for card processing, the merchant is ultimately responsible for ensuring compliance.

Contractual risk transfer to third-party vendors may provide an avenue for eventual indemnification or recovery, but in most cases a merchant must front the direct and indirect expenses, including the possible loss of business. Fortunately, cyber liability insurance is available to cover many of these expenses and provide access to expert risk management services at highly discounted rates.

4 MERCHANT CYBER LIABILITY MYTHS DEBUNKED

Using a third-party card processing vender makes PCI DSS compliance their problem.

No, every merchant is responsible for PCI DSS compliance even if using an outsourced service. If an outsourced payment processing vender is breached, the merchant is liable for the breach and the PCI assessment following the breach!

The Issuing Bank or Credit Card Company is responsible for costs of a Forensic Investigator.

No, all costs of Payment Card Industry Forensic Investigator are the merchant's responsibility

Only large companies are required to maintain PCI DSS Compliance.

No, every company, irrespective of size, that accepts credit card payments must be PCI compliant.

EMV Chip Card compliance means PCI DSSS compliance.

No, being EMV compliant simply demonstrates the merchant's support of PCI DSS requirements but it does not ensure PCI DSS compliance. EMV compliant merchants can still be found liable if they are not PCI DSS compliant.

Along with PCI DSS compliance and the implementation of EMV Chip Card Technology, Point of Sale (POS) encryption and Tokenization can help further lower security risks!

To learn how to best protect your clients' businesses talk to the cyber insurance experts at CRC and Swett & Crawford.

Swett & Crawford

CRC
PERFORMANCE IS THE DIFFERENCE™