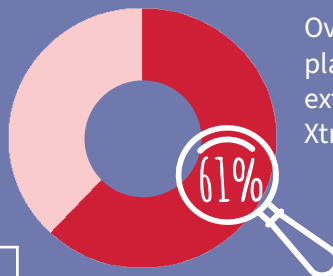# HUMAN RISK

is a big deal, but insiders are far more likely to be **vectors** than villains.

~~VILLIAN~~ HUMAN

Human risk contributes to most incidents

The Cyentia Institute's Information Risk Insights Study (IRIS) 20/20 "Xtreme Edition" analyzes ~100 of the largest cyber loss events of the last 5 years.

Insider misuse (~6 events)
Insider errors (~25 events)
Phishing (18 events)
Credential attacks (46 events)

61%

= $15 BILLION

Overall, observable forms of human risk played a direct role in 63 of the 103 (61%) extreme loss events included in the IRIS Xtreme.
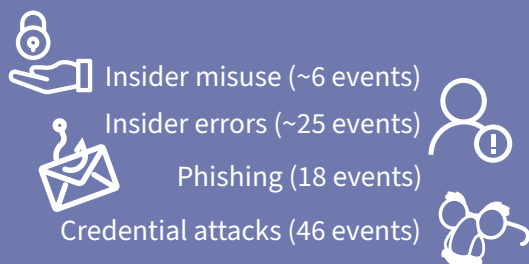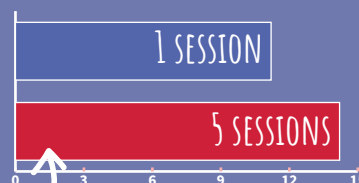
These human risk factors racked up a price tag of $15 billion—that's **88%** of the total losses attributed to the largest cyber incidents of the last five years! The enormity of the human element in cyber risk is clearly something organizations cannot afford to ignore.

HOW TO ADDRESS THE ISSUE OF HUMAN RISK

Too much training can be counterproductive.

11.2% of users who had only one training session clicked on a phishing link, whereas 14.2% of those who had five training sessions clicked on the link.

1 session
5 sessions

0   3   6   9   12   15

Your training doesn't match reality.

Real
Simulated
12am
9am
12pm
5pm

Phishing simulations are sent in the wee hours of the morning, real phishing happens throughout the day.

Equip users for success.

Users with an active password manager are 19x less likely to have a malware incident than those without (0.4% to 7.4%).
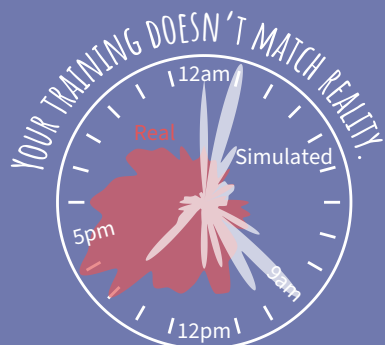
No password manager

With password manager

Know Your Role(s).

Malware infections are 10x more likely to occur among users at the bottom of the org chart than those at the top; when measuring rank-and-file employees, managers and contractors, employees at the bottom rung were again the most likely to click on phishing links.

Read more: https://elevatesecurity.com/resource/cyentia-elevating-human-attack-surface-management/

119
Cyentia INSTITUTE

Elevate Security