THE CYBER CONTINUUM OF INTENT

Grouping Insiders into Intent Types | Many cyber actions that seem routine at first glance can actually decrease the stability of security programs and processes. This makes anyone that touches the network an insider.

The Cyber Continuum of Intent model addresses the relationship between insiders and their cyber activity, lending insight to characteristics and motivations that lead a normal, productive user to the center of a breach.

ACCIDENTAL INSIDER

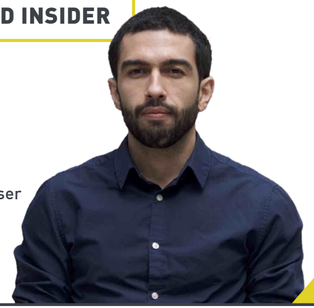
Types

- Inadvertent actors
- Convenience seekers

Possible characteristics

- Poor attention to detail
- Relatively inexperienced with security policies
- High stress levels or inability to cope with job demands
- Maintain a false sense of ownership over company data

COMPROMISED INSIDER



Types

- Malware victims
- Impersonated users

Possible characteristics

- Accesses sensitive data typically never handled by user
- Sends spam and other malware infused email
- Manipulates, alters or destroys data
- Use of peer login credentials

MALICIOUS INSIDER

Types

- Rogue insiders
- Criminal actors

Possible characteristics

- Dissatisfied with role at the organization
- Engages in unethical behavior
- Had a poor performance review or laid off
- Disgruntled with management

Read the full report, "The 2017 State of Cybersecurity"

FORCEPOINT
POWERED BY Raytheon

Protecting the human point.