Insider threats to Cybersecurity

6th CSIR Conference
Darshan Lakha
Vodacom Group
CTSO

6 October 2017
INSIDER THREATS

DATA SECURITY

IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
Are insider threats the main security threat in 2017?

- High Risk Applications: 95%
- Leavers, Joiners & Movers: 56%
- Public Data: 64%
- Inappropriate Internet Usage: 59%
- Security Bypass x2
INSIDER THREATS | Who is involved?

Privileged Users

Terminated Employees

Third Parties
INSIDER THREATS | The danger

According to a 2017 Insider Threat Report, 53 percent of companies estimate remediation costs of $100,000 and more, with 12 percent estimating a cost of more than $1 million.

Insider threats can go undetected for years

Hard to distinguish harmful actions from regular work

Easy for employees to cover their actions

Hard to prove guilt
INSIDER THREATS | The cause

What makes malicious insiders conduct such crimes?

- Acting on opportunity
- Taking revenge for perceived injustice
- Making a statement
- Doing competitor’s bidding
- Seeing themselves as a future competition

Are you satisfied with your current salary?

YES  NO
INSIDER THREATS | Combating it!

Background Checks

General Investigations

Comprehensive Background Investigations

Background Screening Services

Truth Verification

Risk Surveys and Crime Analysis
INSIDER THREATS | Combating it!

Watch employee behaviour
Conduct a privilege audit.

Start all accounts with least privilege.

Enforce the separation of privileges.

Use just in time privileges.

Make individual actions traceable.

Use the Principle Of Least Privilege

POLP
Control user

Unique complex passwords

Prohibit credential sharing

Use two-factor authentication
Use auditing to monitor access to files

Examine cached Web files

Monitor Web access at the firewall

Monitor incoming and outgoing e-mail messages

Control what software employees can install or run
INSIDER THREATS | Combating it!

Obtain C-level support
Partner with key departments
Be relevant
Measure success
Incentivise awareness
Use a variety of awareness tools

Darshan Lakha
5 January 2017
INSIDER THREATS | Conclusion

Follow a good “intake” and “exit” program

Apply and verify “privilege user access management”

Apply “strong security baselines” both inside and externally

Create a monitoring process

Verify by regular audit process

Educate and inform

Know your employees

Who are the “bad guys”?  
45% Outsiders  
31.5% Malicious insiders  
23.5% Inadvertent Actor

Darshan Lakha
Questions?