Cybersecurity & Insider Threats
“It’s not about the 98% you catch, it’s about the 2% you miss.”
Types of Insider Threats

- **Negligent Insiders** - Insiders who accidentally expose data – clumsy or careless employees

- **Malicious Insiders** - Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work

- **Compromised Insiders** - Insiders whose access credentials or computers have been compromised by an outside attacker
Types of Insider Threats

- **Negligent Insiders** - Insiders who accidentally expose data – clumsy or careless employees

- **Malicious Insiders** - Insiders who intentionally steal data or destroy systems – such as a disgruntled employee who deletes some records on his last day of work

- **Compromised Insiders** - Insiders whose access credentials or computers have been compromised by an outside attacker
Insider Threat Motivators

Personal Factors
- Greed or Financial Need
- Anger/Revenge
- Blackmail
- Divided loyalties
- Approval seeking
- Problems at work
- Ideology
- Thrill seeking
- Family problems

Disgruntlement
- Retaliation
- No recognition
- conflicts
- Job dissatisfaction
- pending layoff
- Personal vendetta
- Ego
- Self image
- Irrational behaviour
- Divorce/Separation
Qualities of an Insider

Respectable

TRUSTWORTHY

Access All Areas

Astute

Employee of the Month
Who Are the Insiders?
Managers pose the greatest insider threat, at 59%, according to respondents, followed by contractors and consultants (48%) and regular employees (46%).
**Who Are the Insiders?**

Managers pose the greatest insider threat, at 59%, according to respondents, followed by contractors and consultants (48%) and regular employees (46%).

**Few Have Appropriate Controls**

30% of respondents said their organization lacks appropriate controls to prevent insider attacks, 23% are not sure, but 47% said they do have appropriate controls.
Who Are the Insiders?
Managers pose the greatest insider threat, at 59%, according to respondents, followed by contractors and consultants (48%) and regular employees (46%).

Few Have Appropriate Controls
30% of respondents said their organization lacks appropriate controls to prevent insider attacks, 23% are not sure, but 47% said they do have appropriate controls.

Risky Users
The top five users who pose insider threats are:
- Privileged users: 59%
- Contractors/consultants and temporary workers: 48%
- Regular employees: 46%
- IT administrators and staff: 41%
- Third-party service providers: 30%
Who Are the Insiders?
Managers pose the greatest insider threat, at 59%, according to respondents, followed by contractors and consultants (48%) and regular employees (46%).

Few Have Appropriate Controls
30% of respondents said their organization lacks appropriate controls to prevent insider attacks, 23% are not sure, but 47% said they do have appropriate controls.

Risky Users
The top five users who pose insider threats are:
- Privileged users: 59%
- Contractors/consultants and temporary workers: 48%
- Regular employees: 46%
- IT administrators and staff: 41%
- Third-party service providers: 30%
Survey: One-Third of Employees Would Sell Corporate Information for the Right Price

Vormetric: 93% of companies face insider threat cybersecurity risks

Insider threats from privileged users cause anxiety, but contractors could prove to be worse.

58% Information Security Incidents Attributed to Insider Threat

14 APR 2015 NEWS

92% of Healthcare IT Admins Fear Insider Threats

Jeep hacker: I’m more afraid of texting and driving

Hackers are selling your data on the ‘dark web’... for only $1