RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SOP-W06

# The Ticking Time Bomb of Insider Threat

**Rashmi Knowles CISSP**

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi

# Agenda

- Reality of Insider Threat
- Types of Insider Threat
- The Human Factor
- Ten Step Mitigation Strategy
- Q&A

# People are the New Perimeter

# Insider Threat

- Insiders who maliciously or accidentally do things to put an organisation and its data at risk
- Perpetrated by employees, outsiders who have stolen valid user credentials, business partners, contractors with inappropriate access rights, third party service providers with excessive admin privileges

Higher risk of Malicious Insider Attack = Intrinsic Factors (personality) + extrinsic factors (opportunity/motivation/events)

# Who Can You Trust Anymore?

- 37% of attacks by Malicious Insiders
- 85% of attacks include Insider and Privilege misuse on Corporate Networks
- Human error causes of 66% of data breaches
- Insider Threat ranked 2nd hardest to solve by US Government

Source Verizon DBIR 2014

# Employees are the Most Cited Culprits

- According to 32% of respondents Insider Crime was more costly or damaging than incidents perpetrated by outsiders
- 75% of respondents do not involve law enforcement or bring legal charges in compromises committed by insiders
- Current Employees 35%, Former employees 30%, Current providers 18%, Former providers 15%, Customers 11%

Source pwc.com/gsiss2015

# Who Can You Trust Anymore?

- Edward Snowden
- Sony
  - “sympathetic insider or insiders aided them in their operation and that they were seeking equality”
- Target
  - Credentials used from an HVAC company working for Target

# What if you had a ‘Snowden’?

- Would you know what was actually taken?
- What documents and systems were accessed?
- How long would it take you to find out?
- Who perpetrated it?
- Do you have an incident response plan?
- Can you follow a forensics trail?

# Addressing Different Threats

Malicious Insider

Accidental Insider

UIT

Visibility

Analysis

Action

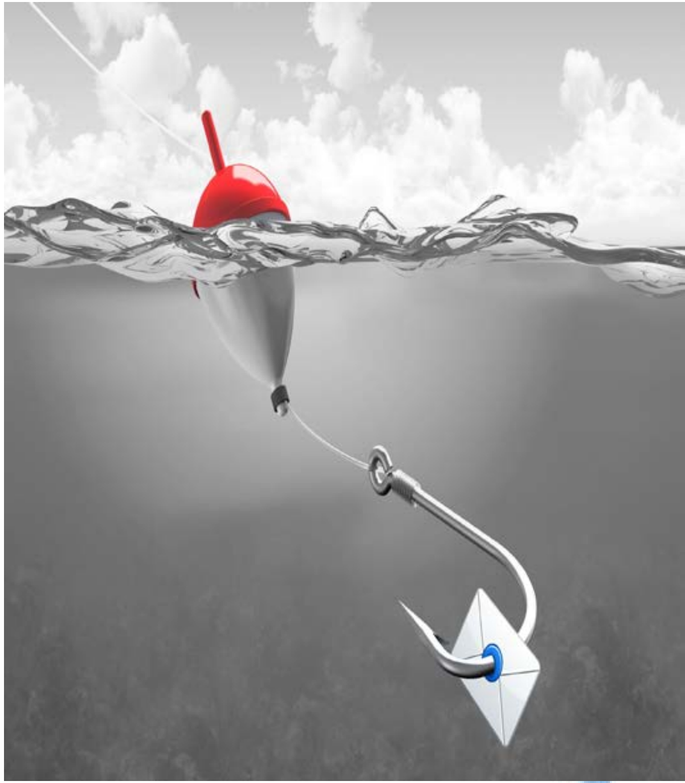
Visibility

Analysis

Education

# The Human Factor

- Social engineering
- Phishing/spear phishing
- Malware
- Website exploits
- Mobile Apps

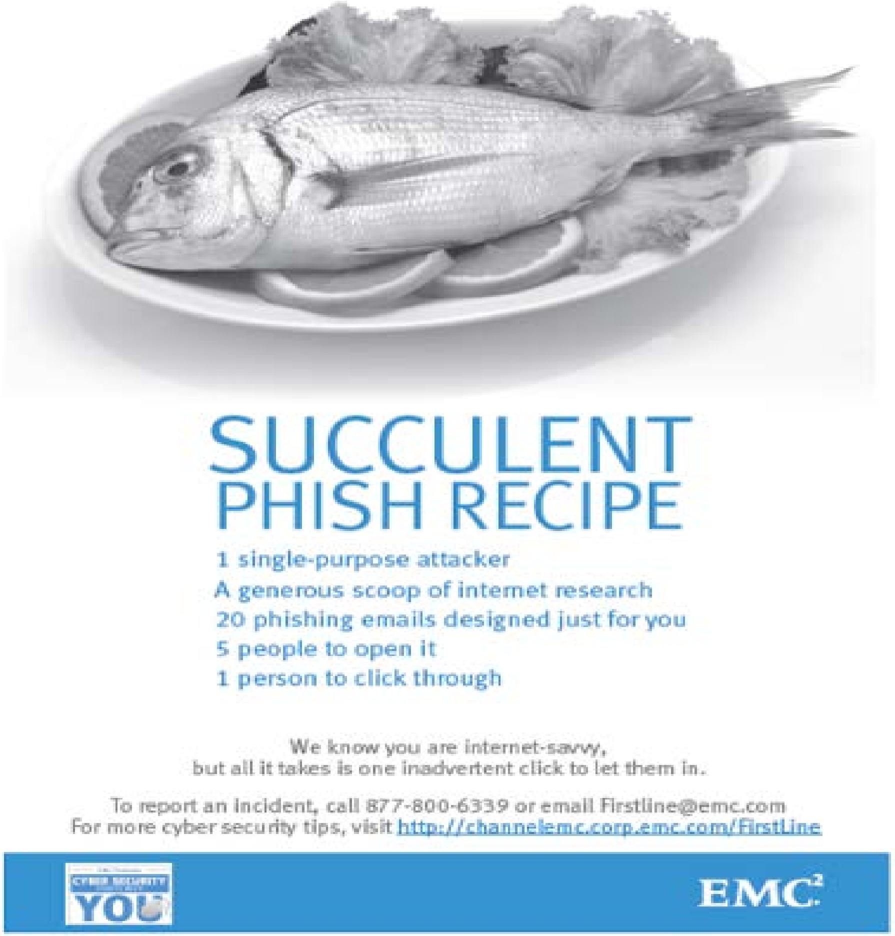


# Education

- Boring, out-of-context, too long
- Limited user interaction or motivation
- Security team competency is not education
- Limited measurement, feedback and continuous improvement

# Training has a Big Role to Play

- Lack of understanding
- Wide range of scenarios
- Required knowledge is vast & growing
- Practical strategies not easy to articulate
- Security is a secondary task
- Delivery methods must be compelling
- According to ISSA Middle East lags behind compared to US and Europe



# SUCCULENT PHISH RECIPE

1 single-purpose attacker
A generous scoop of internet research
20 phishing emails designed just for you
5 people to open it
1 person to click through

We know you are internet-savvy,
but all it takes is one inadvertent click to let them in.

To report an incident, call 877-800-6339 or email Firstline@emc.com
For more cyber security tips, visit http://channelemc.corp.emc.com/FirstLine

CYBER SECURITY
YOU
EMC²

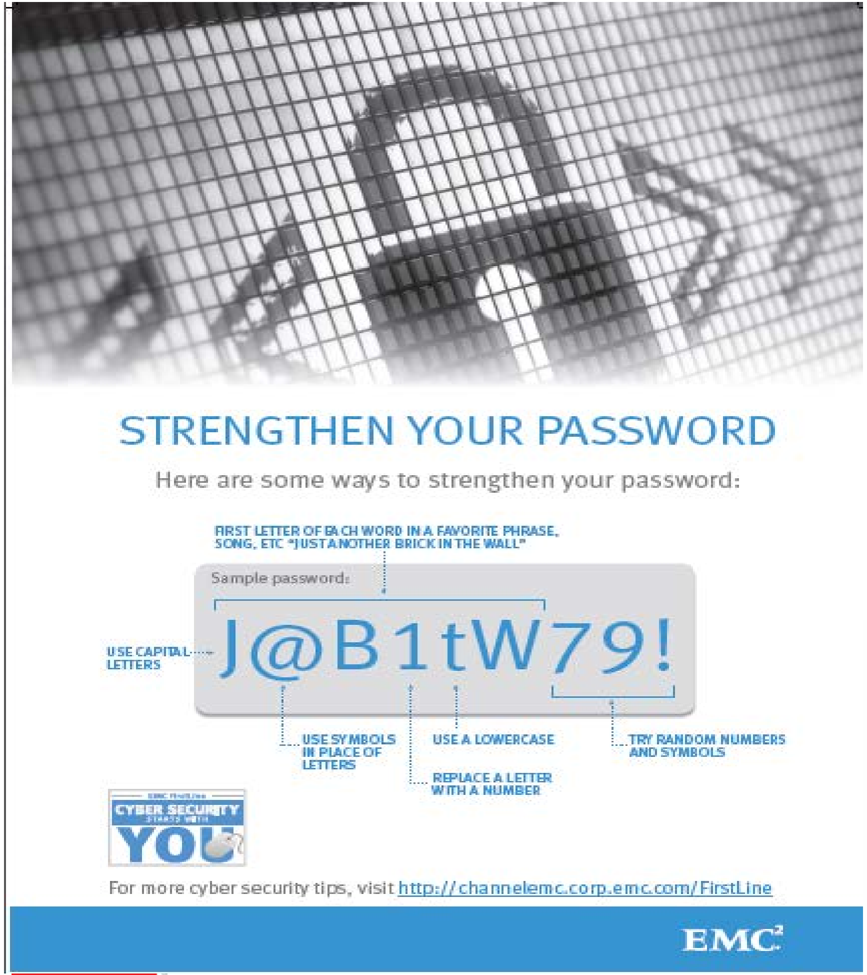
## SOME IMPERSONATORS ARE EASY TO SPOT.
# OTHERS ARE NOT.

You may be Internet-savvy, but all it takes is one inadvertent click to let a virus in, compromise your computer, your personal information or EMC systems:

- Never trust a link without verifying its destination.
- Inspect links carefully before clicking.
- Open a web browser and type the URL instead.

EMC FirstLine
THINK
BEFORE YOU CLICK

To report an incident, call 877-800-6339 or email FirstLine@emc.com
For more cyber-security tips visit http://channelemc.corp.emc.com/FirstLine



## STRENGTHEN YOUR PASSWORD

Here are some ways to strengthen your password:

FIRST LETTER OF EACH WORD IN A FAVORITE PHRASE, SONG, ETC "JUST ANOTHER BRICK IN THE WALL"

Sample password:

J@B1tW79!

USE CAPITAL LETTERS

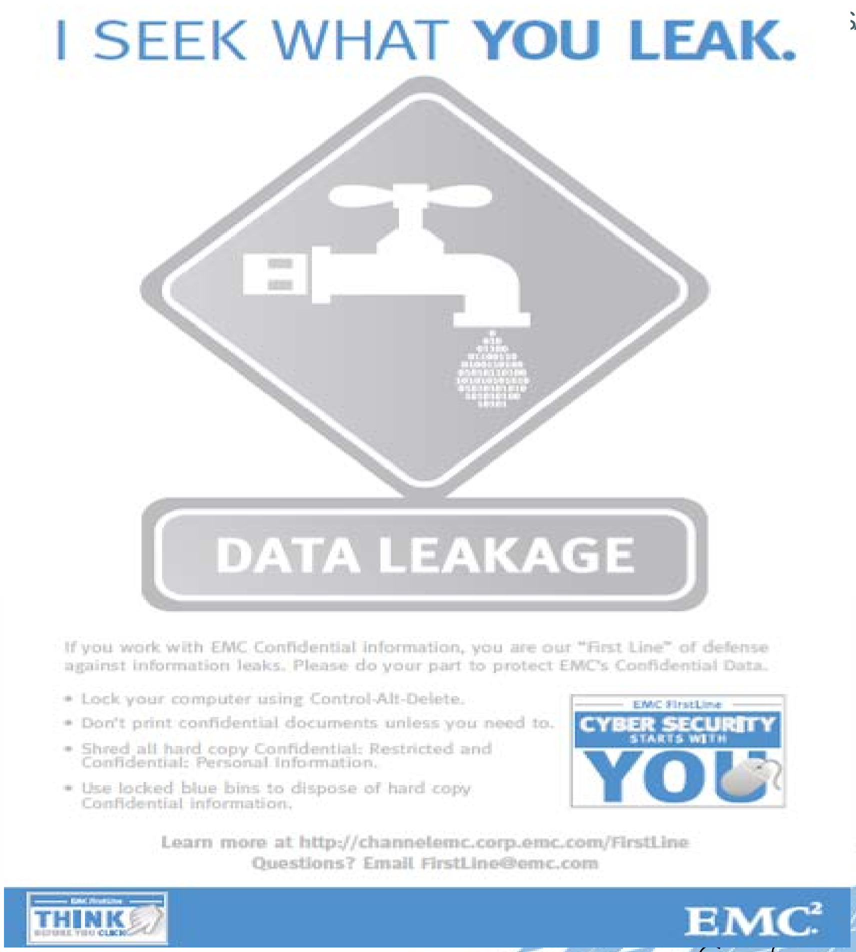
USE SYMBOLS IN PLACE OF LETTERS

USE A LOWERCASE

REPLACE A LETTER WITH A NUMBER

TRY RANDOM NUMBERS AND SYMBOLS

For more cyber security tips, visit http://channelemc.corp.emc.com/FirstLine



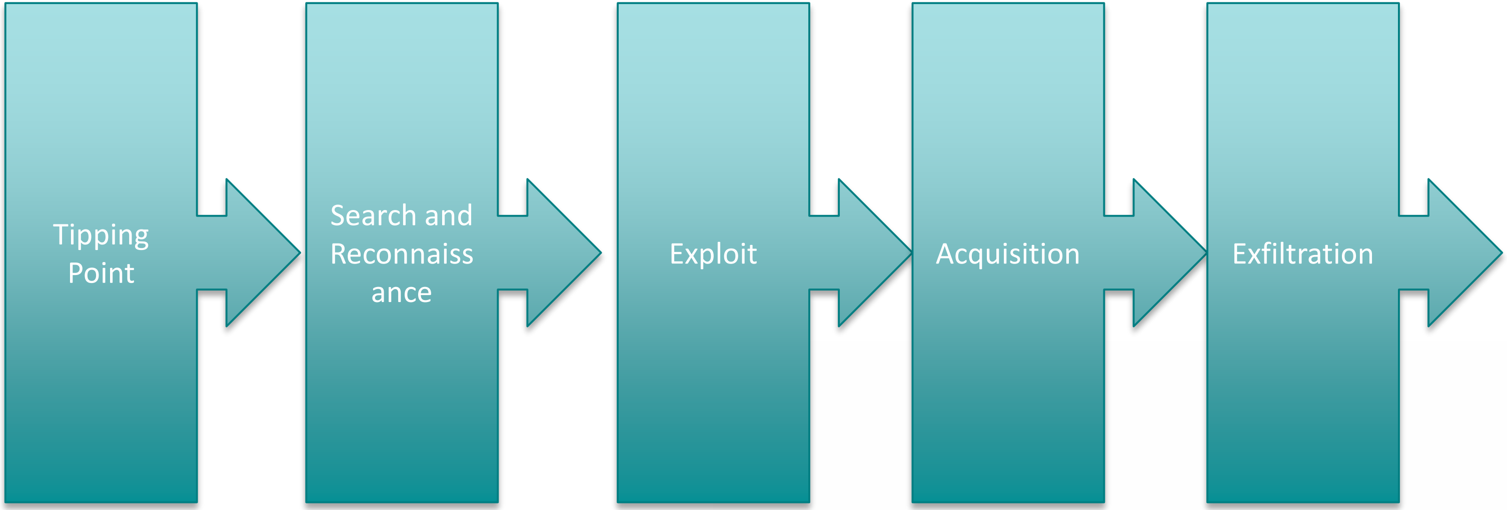
## I SEEK WHAT YOU LEAK.

If you work with EMC Confidential information, you are our "First Line" of defense against information leaks. Please do your part to protect EMC's Confidential Data.

- Lock your computer using Control-Alt-Delete.
- Don't print confidential documents unless you need to.
- Shred all hard copy Confidential: Restricted and Confidential: Personal Information.
- Use locked blue bins to dispose of hard copy Confidential information.

Learn more at http://channelemc.corp.emc.com/FirstLine
Questions? Email FirstLine@emc.com

# The Malicious Insider Threat Kill Chain Phases



Break the chain – Deter, Deny, Disrupt, Degrade, Deceive, Defeat

# The New Security World

It will become increasingly difficult to secure infrastructure

We must focus on **people**, the **flow of data** and on **transactions**

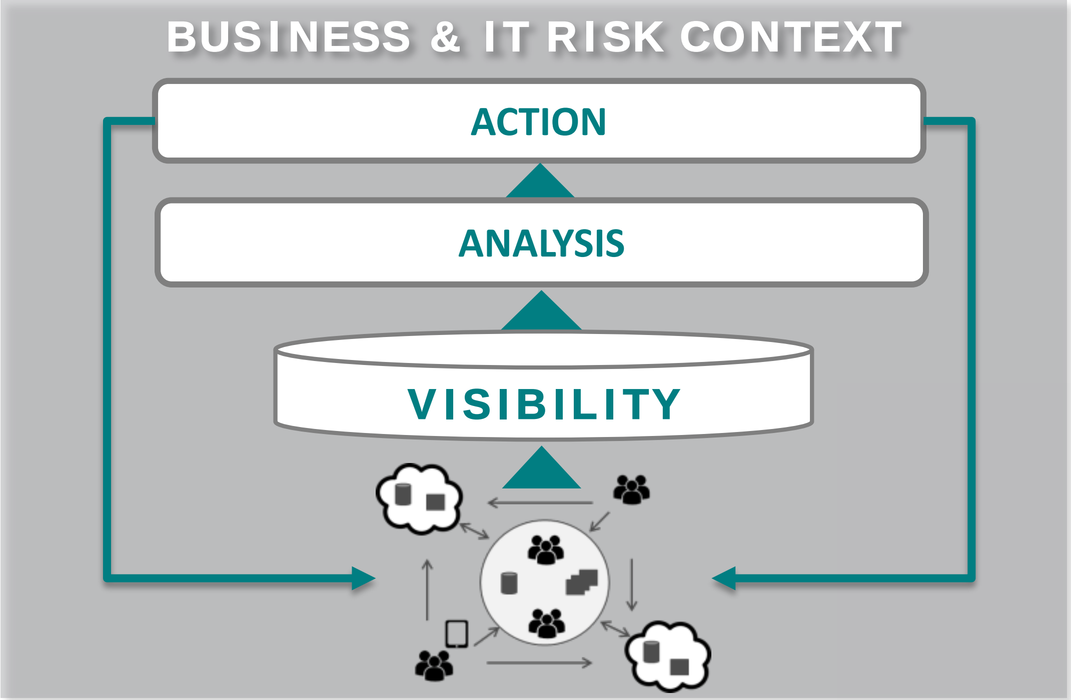
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

#RSAC

# Ten Steps for Mitigating Insider Threat

# Long Term Goal



Act to mitigate
business damage or loss

Detect anomalies
that indicate risks or
threats

Collect data about what matters
Identities - Flow of Data -
Transactions

# 10 Practical Steps

1. Recognise the Threat
   - Champion support to build a mitigation strategy
2. Establish a Baseline for Security
   - Prerequisite for any mitigation program
3. Incident Response
   - Extend existing plans to include malicious insider incidents
   - Work with legal to clearly define a process

# 10 Practical Steps

4. Communication and Awareness
    - Establish, Communicate and enforce AUP
    - Introduce insider-threat awareness training programme
    - Educate employees to recognise the threat and respond

5. Identify Critical Assets
    - MUST be your starting point for any IS programme
    - Document location and flow of sensitive data
    - Monitor systems processing this data

# 10 Practical Steps

6. Access Control
   - Start with least privileged entitlement for access to systems
   - Segregation of duties enforced
   - Access management
   - Focus on elevated privileges/access to critical assets
7. Vetting
   - Vetting process for new personnel
   - Consider including third parties
   - Focus on those who will have access to critical assets

# 10 Practical Steps

8. Data Loss Prevention
   - DLP and IRM for sensitive data exfiltration
   - Use Honey tokens to detect their discovery in unauthorised locations

9. Monitoring
   - SIEM as a minimum requirement
   - Log and event management

# 10 Practical Steps

10. Security Analytics
    - Harvest richer data sets for Insider Threat
    - Complete visibility with logs, full packet netflow and endpoint
    - Behavioural data
    - Contextual data analysis
    - Personal event data from HR
    - Automation of policies and procedures and remediation
    - Data analytics for prediction and diagnosis of threats

# How Can You Apply This?

- Create a long term plan to combat Insider Threat
  - Full visibility, contextual analysis, behaviour monitoring and actionable intelligence
- Identify the gaps and look to fill them in the short-term
- Prioritise the Ten steps for your business
- Implement User education and awareness program

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: SOP-W06

# Thank You

**Rashmi.Knowles@emc.com**

Chief Security Architect
RSA, The Security Division of EMC
@KnowlesRashmi