RSAConference2015

Singapore | 22-24 July | Marina Bay Sands

CHANGE

Challenge today's security thinking

SESSION ID: SPO-R08

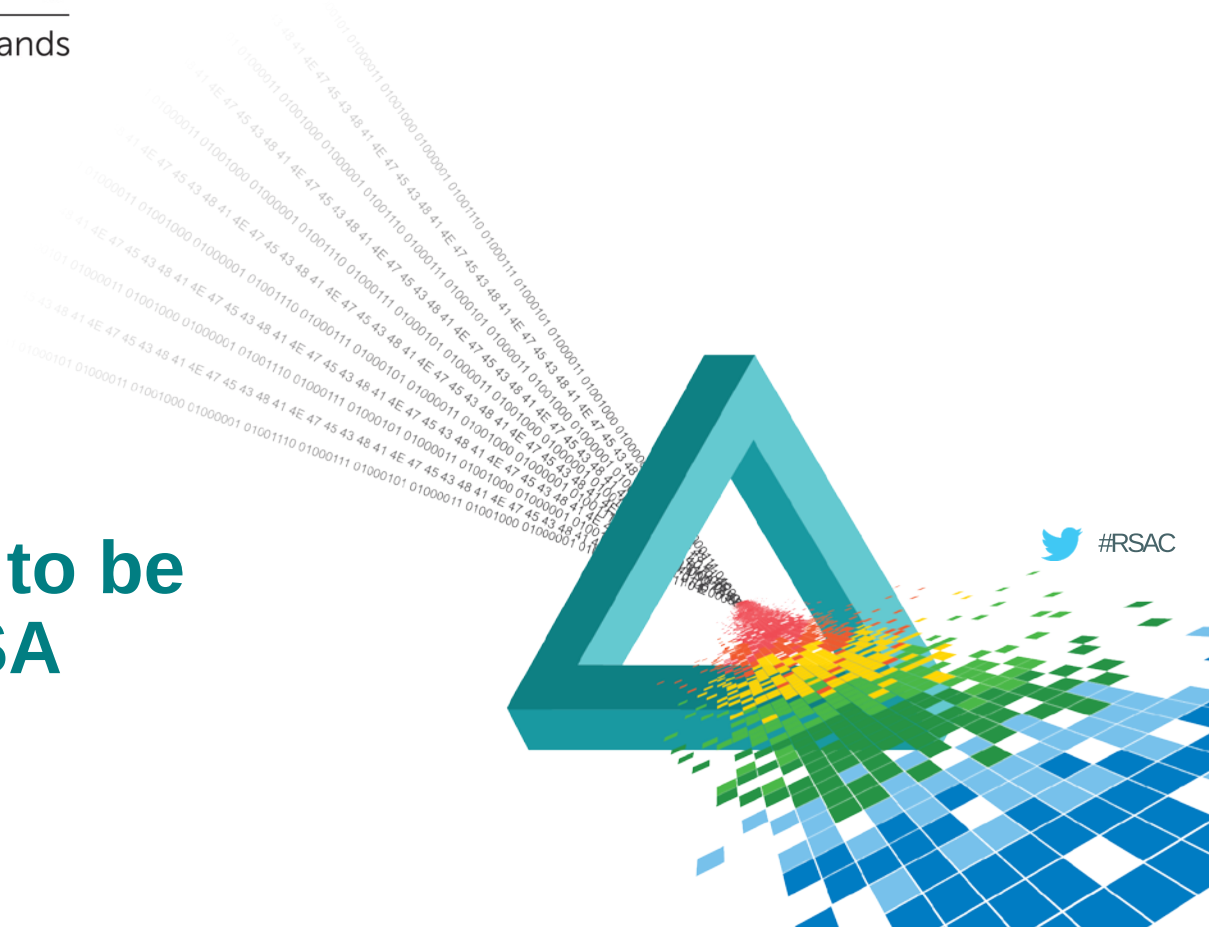
Understanding the Data Breaches of 2014:
Did it have to be this way?

Patrick Grillo

Senior Director, Product Strategy
Fortinet

RSAConference2015

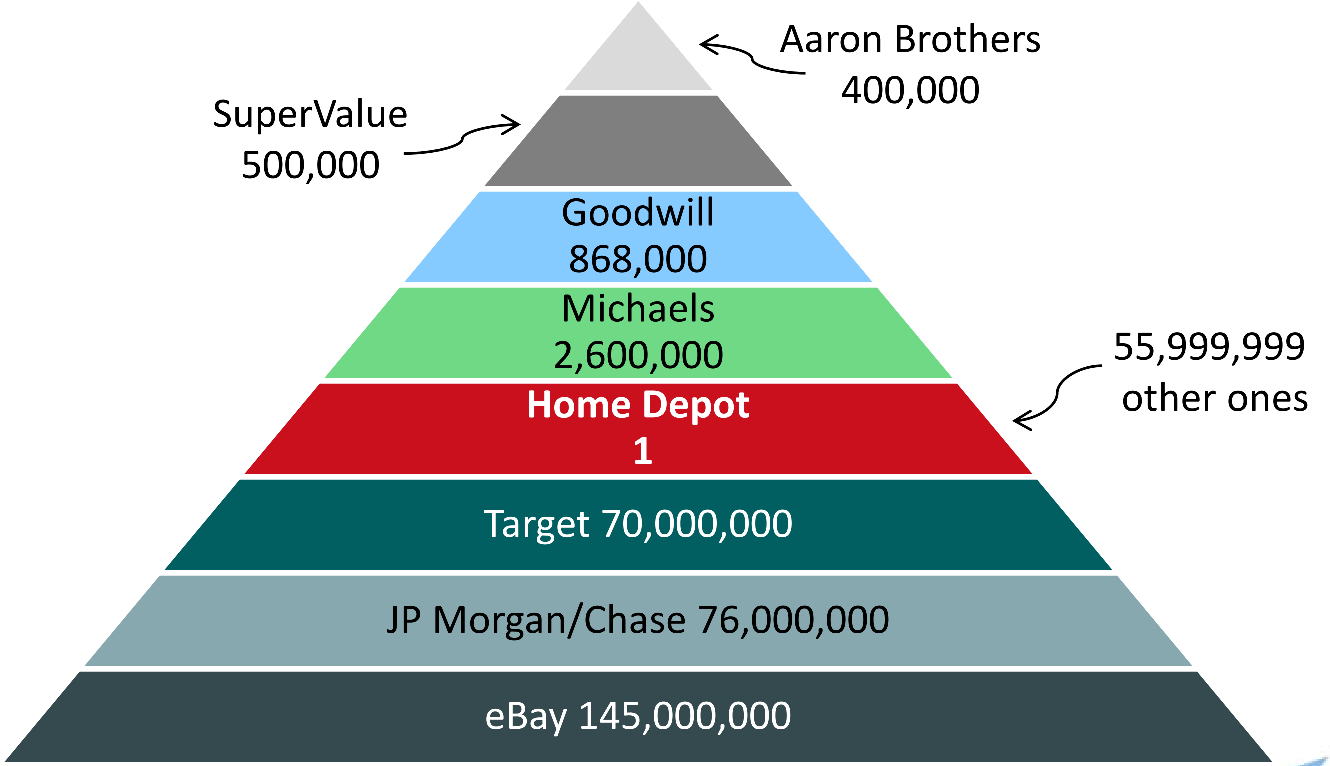
Singapore | 22-24 July | Marina Bay Sands



#RSAC

Embedded Video to be placed here at RSA

Anyone Want To Add Anything?



Aaron Brothers 400,000

SuperValue 500,000

Goodwill 868,000

Michaels 2,600,000

Home Depot 1

55,999,999 other ones

Target 70,000,000

JP Morgan/Chase 76,000,000

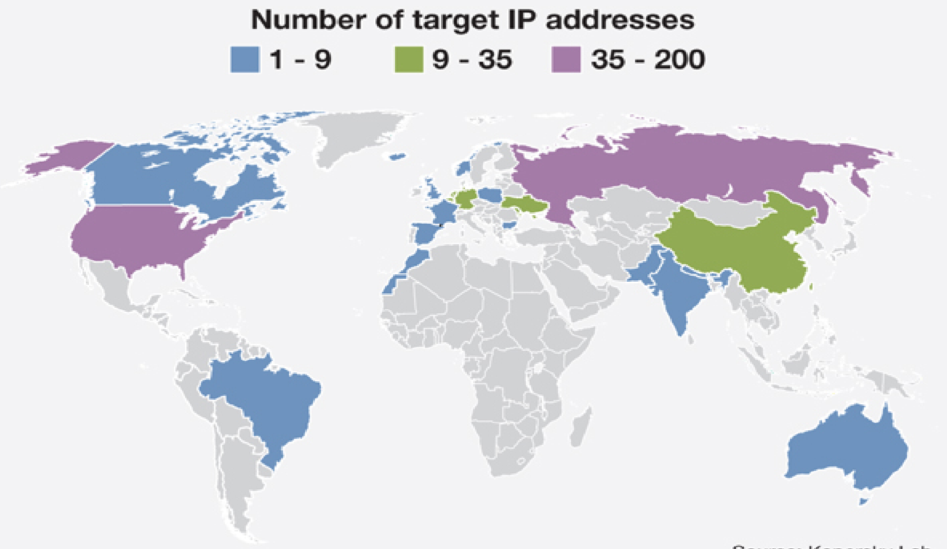
eBay 145,000,000

***Milton Security**

21st Century Bank Robbery

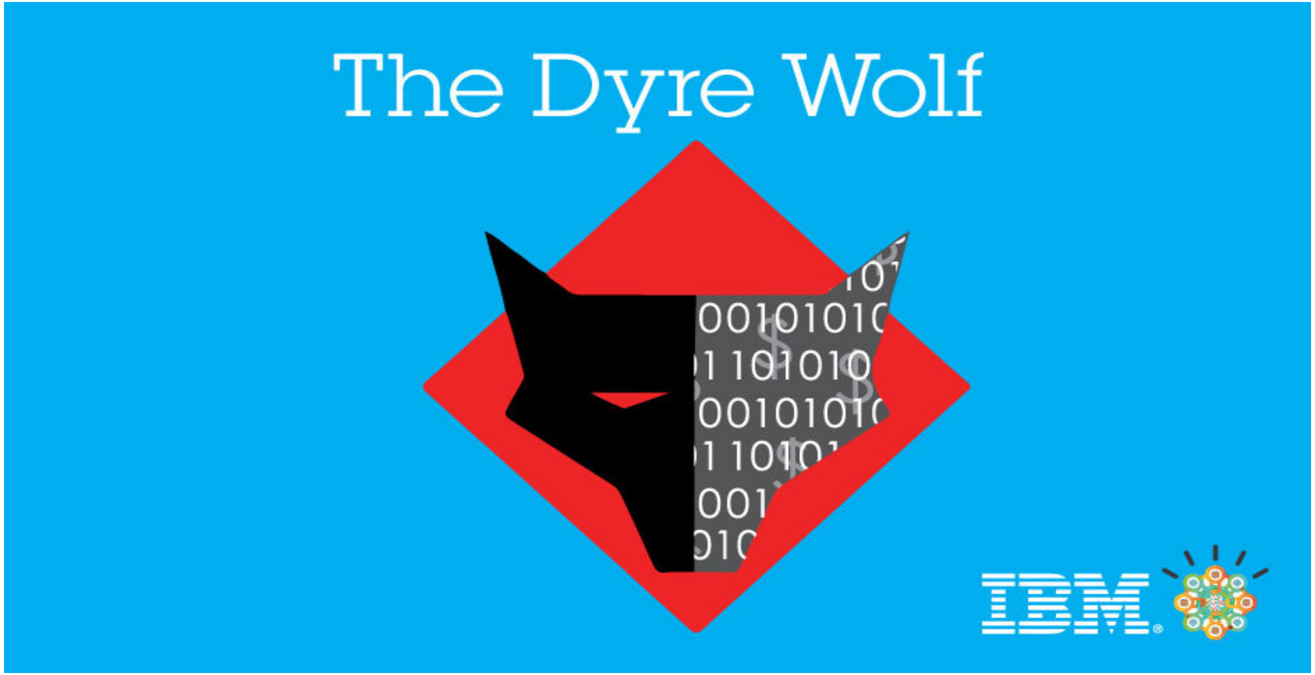
Global Heist

The Carbanak hackers are believed to have hit as many as 100 financial institutions in almost 30 countries

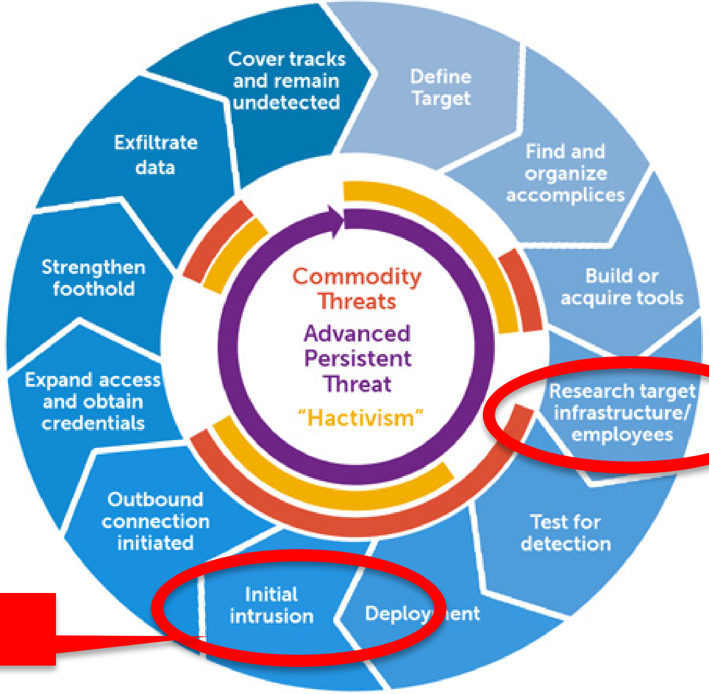


Source: Kapersky Lab

Not Just in the Game of Thrones



Advanced Persistent Threat Structure

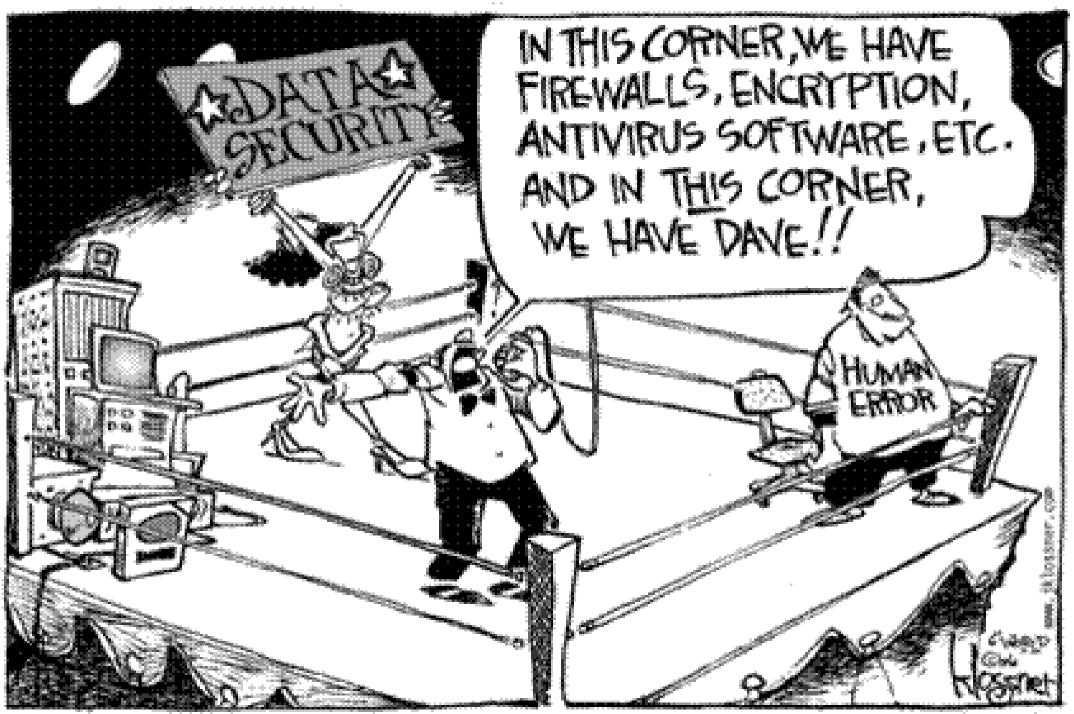

Define Target
Find and organize accomplices
Build or acquire tools
Research target infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen foothold
Exfiltrate data
Cover tracks and remain undetected
Commodity Threats
Advanced Persistent Threat
"Hactivism"

Social Engineering

HOW?

*Wikipedia Commons

Exploiting the Weak Link


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR

The Common Thread

Target:
Outside contractor clicks on phishing email

http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p2

http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

JP Morgan/Chase:
Stolen employee credentials

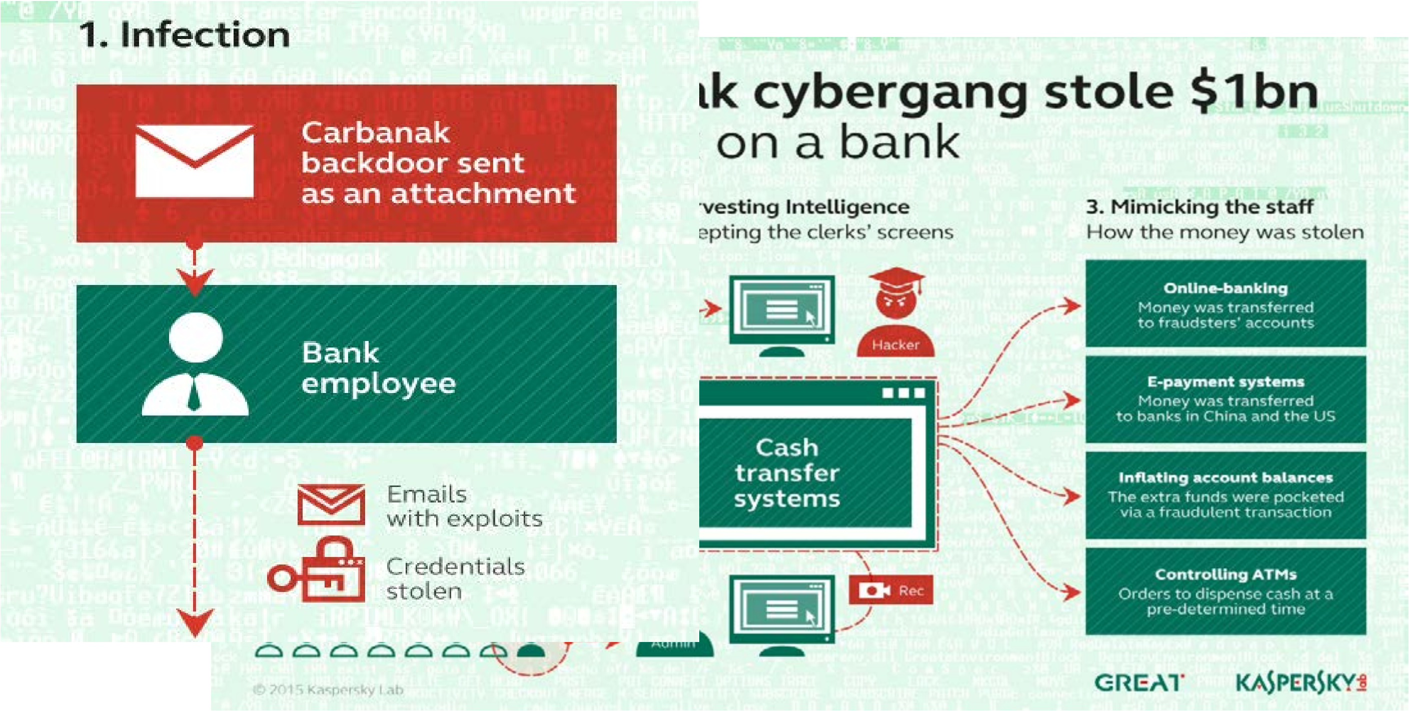
http://www.computerworld.com/article/2862578/twofactor-authentication-oversight-led-to-jpmorgan-breach-investigators-reportedly-found.html

Home Depot:
Stolen login credentials from Third party vendor

http://krebsonsecurity.com/2014/11/home-depot-hackers-stole-53m-email-addreses/

http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html

Cyber Crime on a Global Basis



1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

ık cybergang stole $1bn on a bank

ˈvesting Intelligence

epting the clerks' screens

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

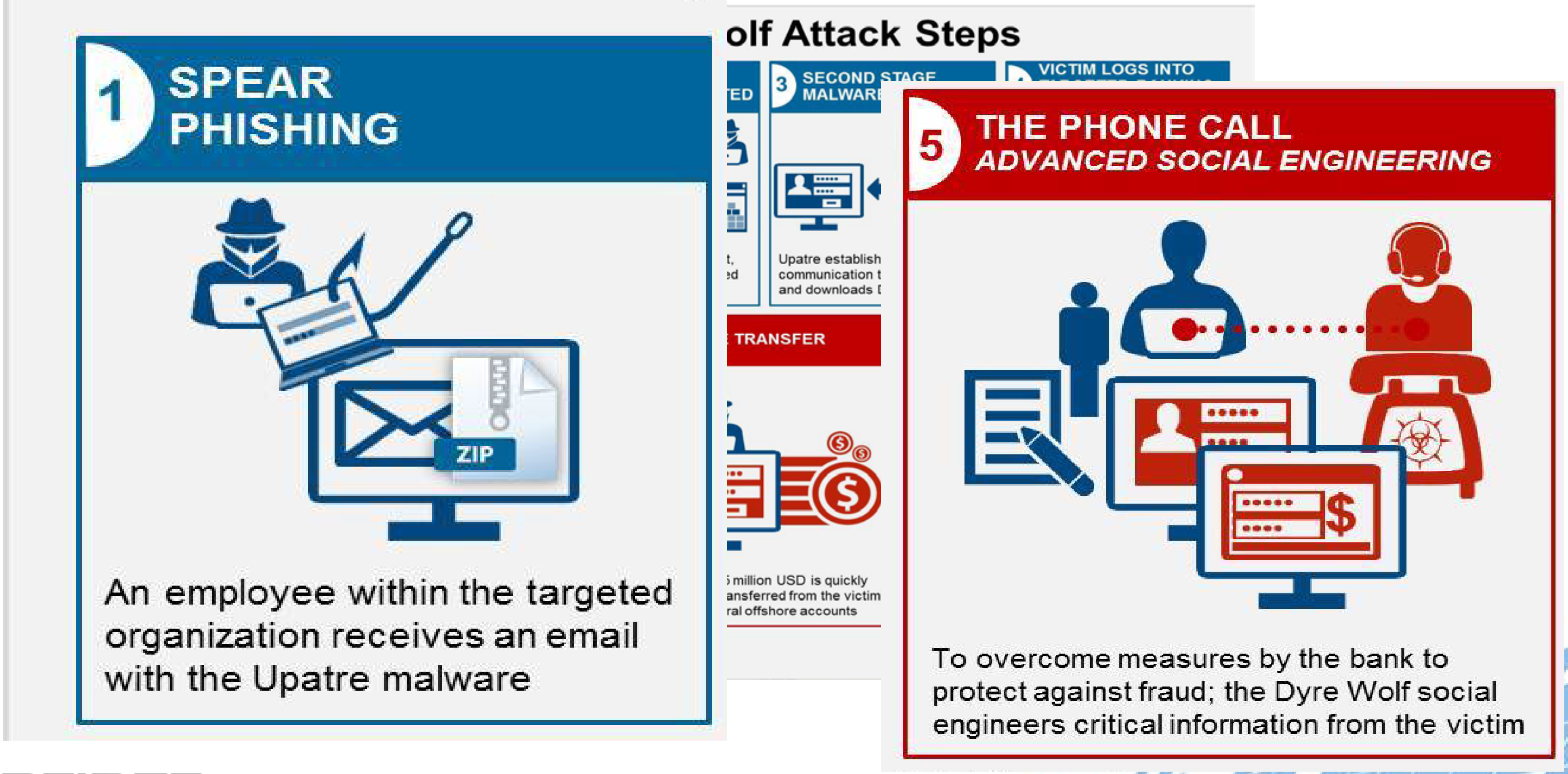
Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

© 2015 Kaspersky Lab

GREAT KASPERSKY lab

Not Just for Consumers



olf Attack Steps

1 SPEAR PHISHING

An employee within the targeted organization receives an email with the Upatre malware

ED

t,
ed

3 SECOND STAGE MALWARE

Upatre establish
communication t
and downloads D

VICTIM LOGS INTO

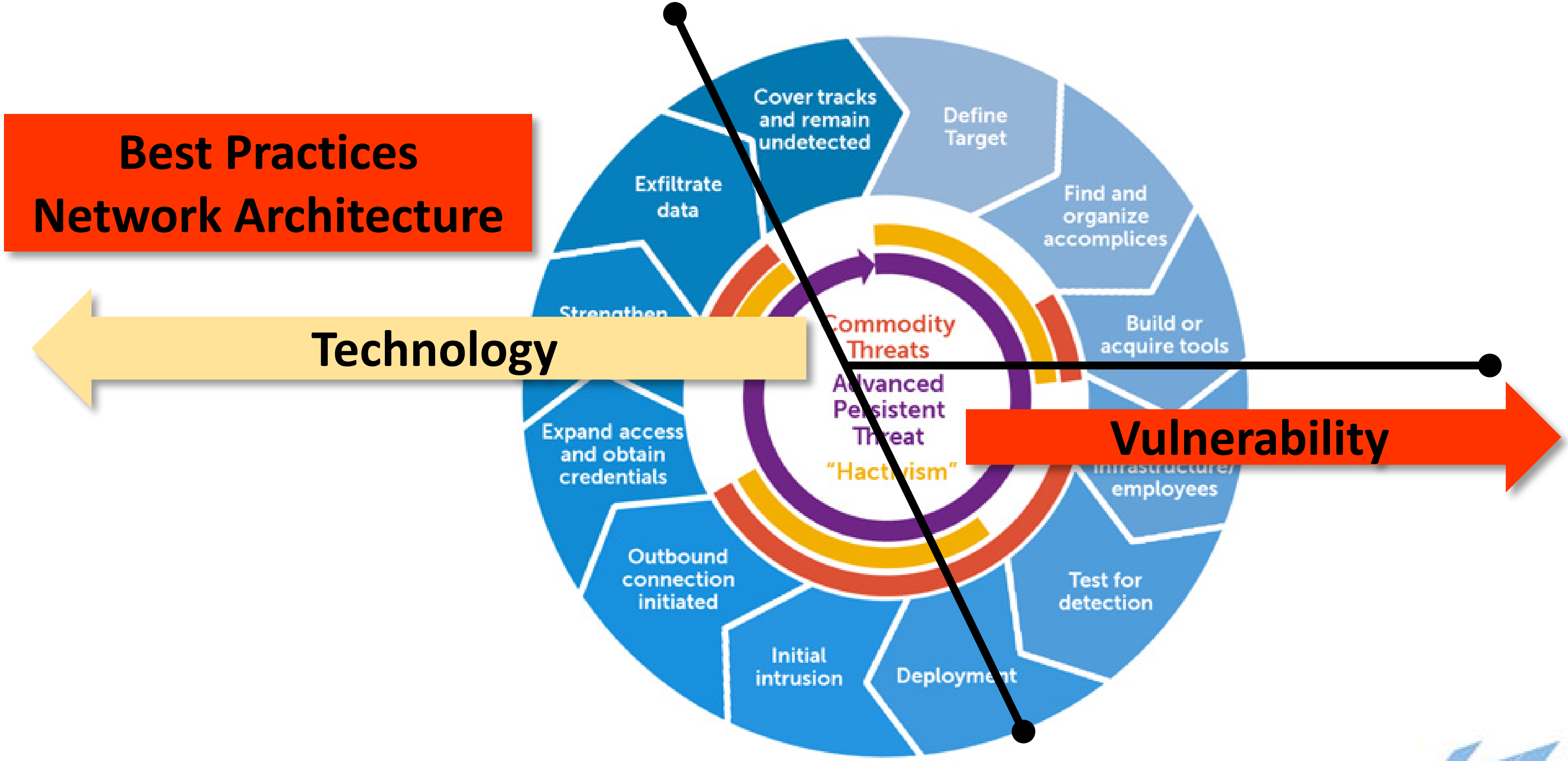
TRANSFER

million USD is quickly
ansferred from the victim
ral offshore accounts

5 THE PHONE CALL
ADVANCED SOCIAL ENGINEERING

To overcome measures by the bank to protect against fraud; the Dyre Wolf social engineers critical information from the victim

Let’s Take a Closer Look



Best Practices
Network Architecture

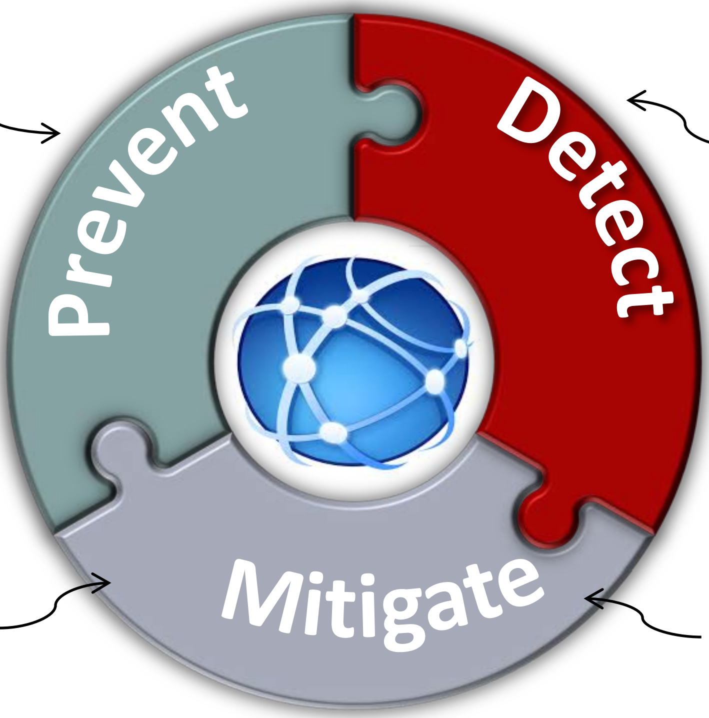
Technology

Vulnerability

Cover tracks and remain undetected
Define Target
Find and organize accomplices
Build or acquire tools
infrastructure/ employees
Test for detection
Deployment
Initial intrusion
Outbound connection initiated
Expand access and obtain credentials
Strengthen
Exfiltrate data
Commodity Threats
Advanced Persistent Threat
“Hactivism”

The Technology Side of Things

Two Factor Authentication
Anti-Virus
Intrusion Prevention
Secure Email Gateway
Web Application Firewall
End Point Protection

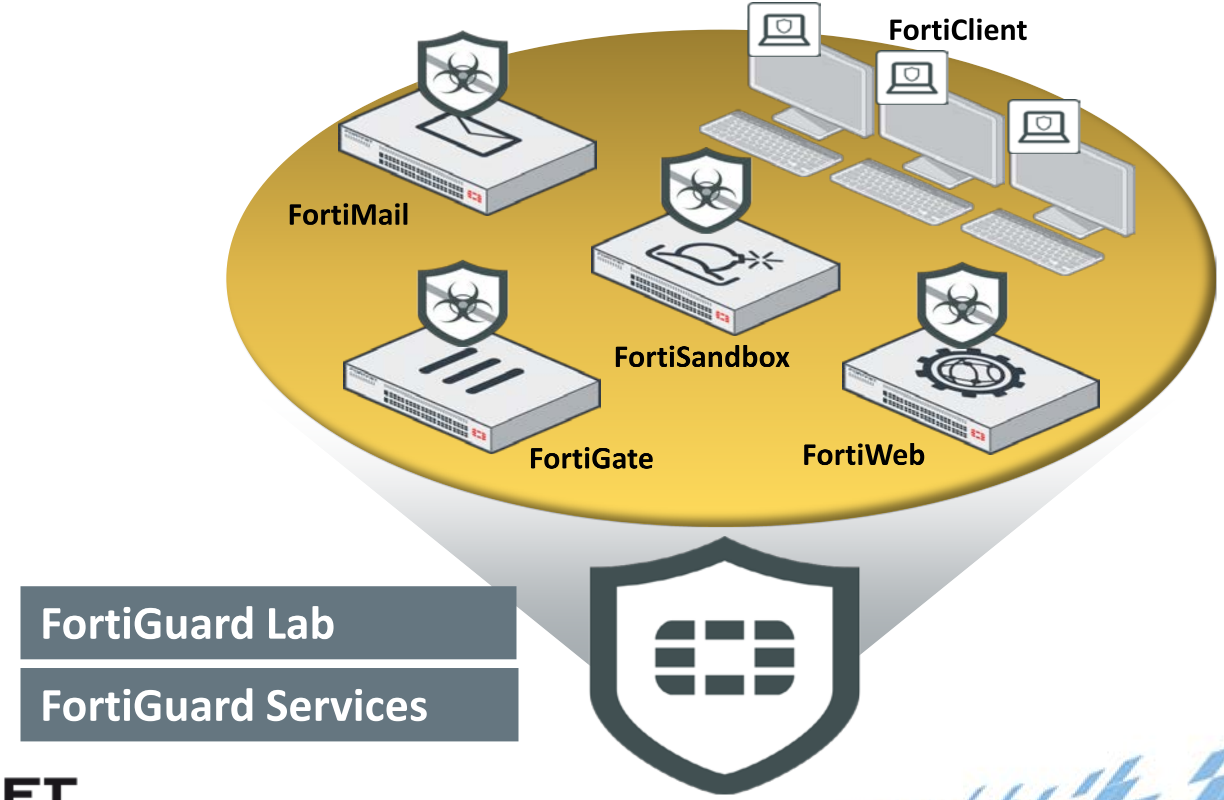


Botnet Detection
IP & Client Reputation
Sandboxing

People
Process
Technology

Threat Intelligence
Zero Day Research
Continuous updates

Advanced Threat Protection



Protecting Deeper Into the Network

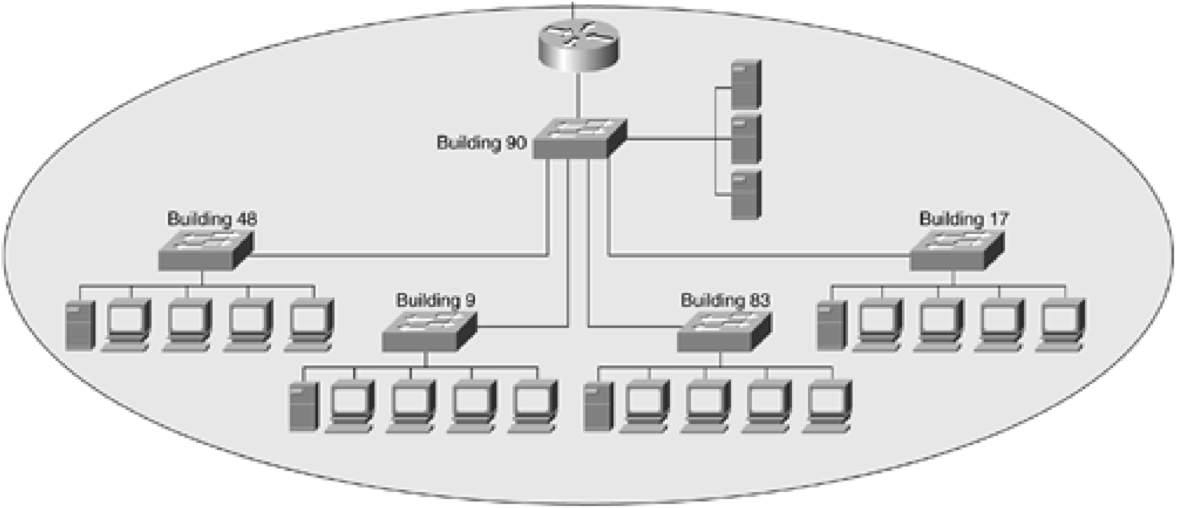
"Oh, hey! I just love these things! ... Crunchy on the outside and a chewy center!"

The European Information Security Summit 2015
hp
THE EUROPEAN INFORMATION SECURITY SUMMIT

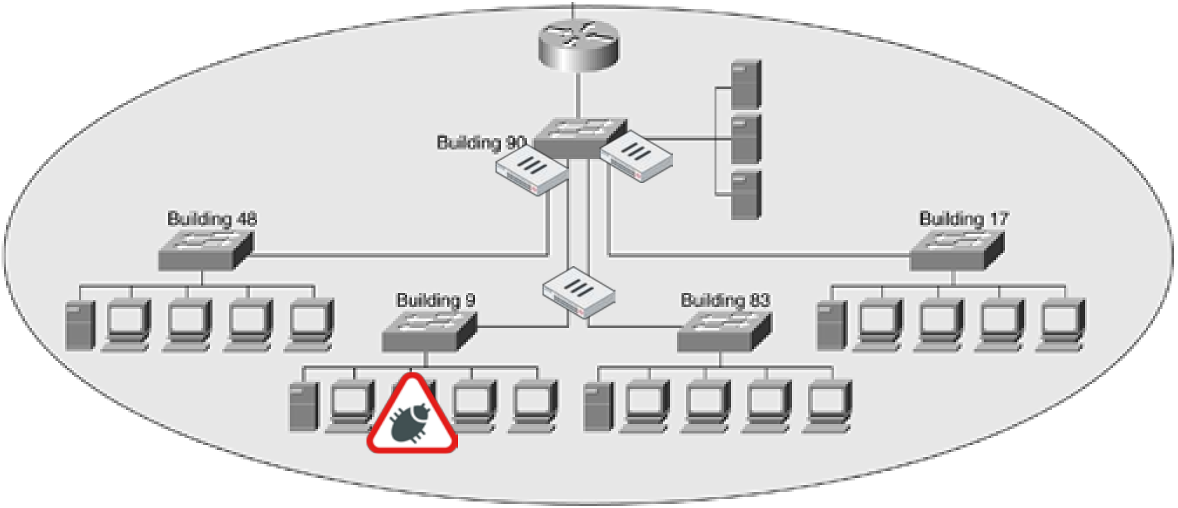
#TEISS15: How to control shadow IT initiatives

What do Igloos and the networks have in common? Patrick Grillo, senior director of solutions marketing at Fortinet, says “they…

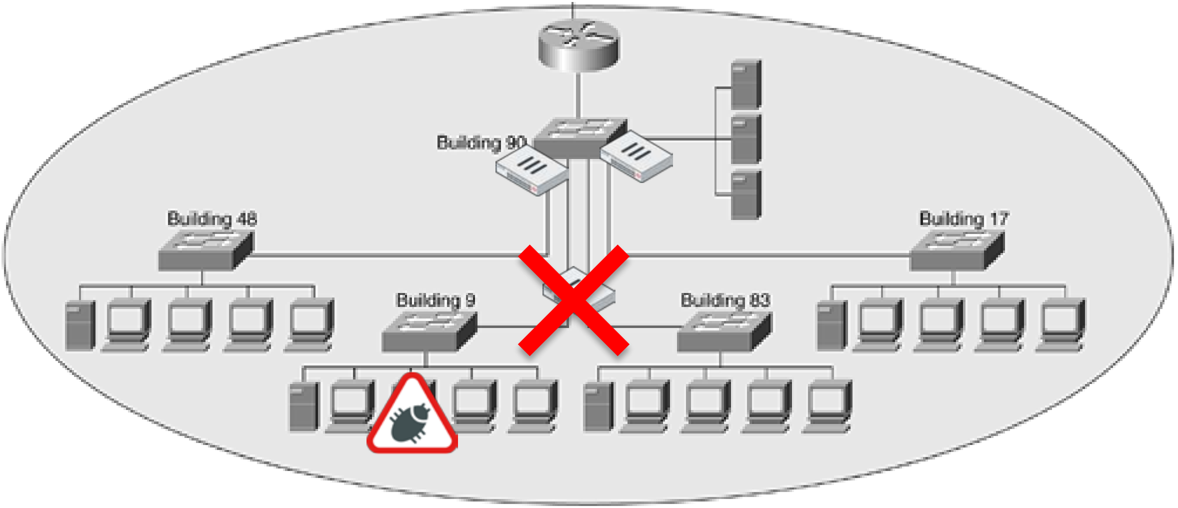
Internal Segmentation For Greater Control



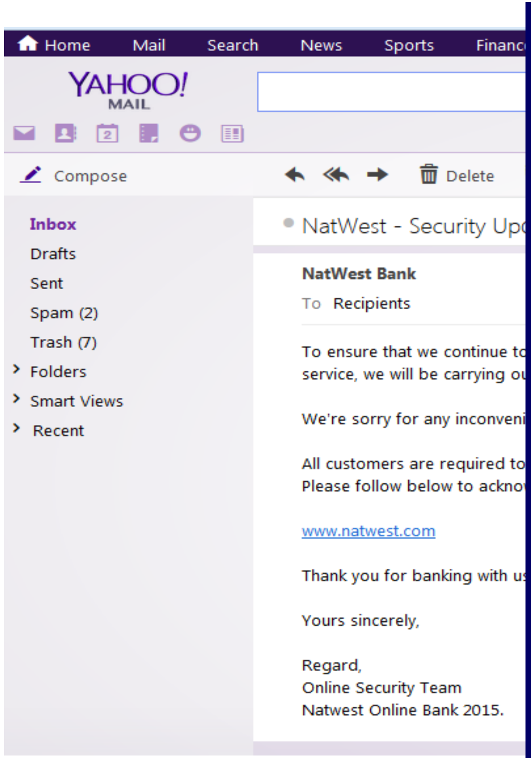
Internal Segmentation For Greater Control



Internal Segmentation For Greater Control



So What Do We Do With Dave?



NatWest - Security Upd

NatWest Bank

To Recipients

To ensure that we continue to
service, we will be carrying ou

We're sorry for any inconveni

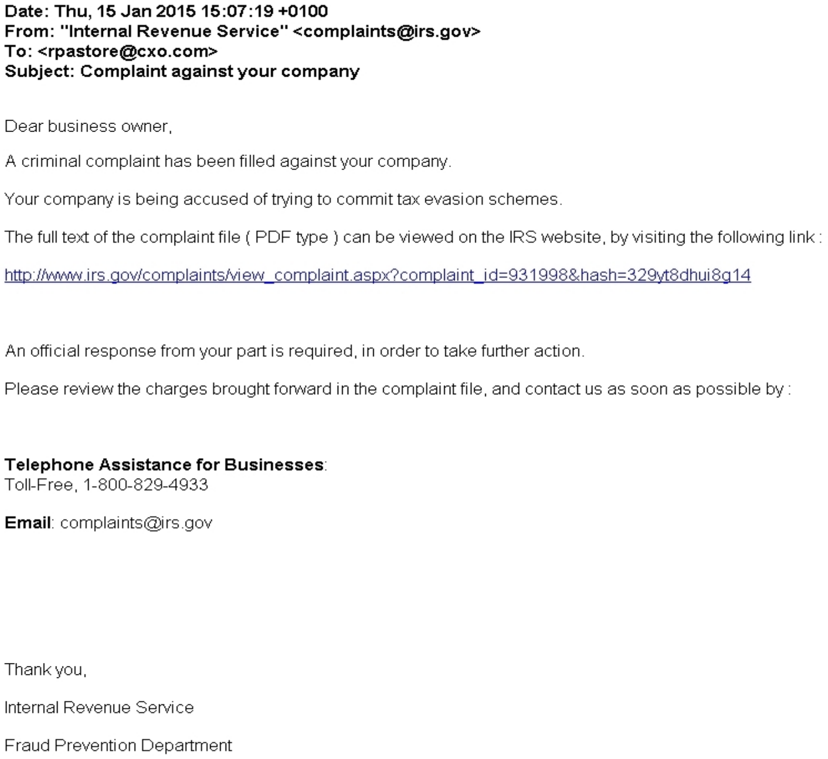
All customers are required to
Please follow below to ackno

www.natwest.com

Thank you for banking with u

Yours sincerely,

Regard,
Online Security Team
Natwest Online Bank 2015.



Date: Thu, 15 Jan 2015 15:07:19 +0100
From: "Internal Revenue Service" <complaints@irs.gov>
To: <rpastore@cxo.com>
Subject: Complaint against your company

Dear business owner,

A criminal complaint has been filled against your company.

Your company is being accused of trying to commit tax evasion schemes.

The full text of the complaint file (PDF type) can be viewed on the IRS website, by visiting the following link :

http://www.irs.gov/complaints/view_complaint.aspx?complaint_id=931998&hash=329yt8dhui8g14

An official response from your part is required, in order to take further action.

Please review the charges brought forward in the complaint file, and contact us as soon as possible by :

Telephone Assistance for Businesses:
Toll-Free, 1-800-829-4933

Email: complaints@irs.gov

Thank you,

Internal Revenue Service

Fraud Prevention Department

Training To Raise Awareness

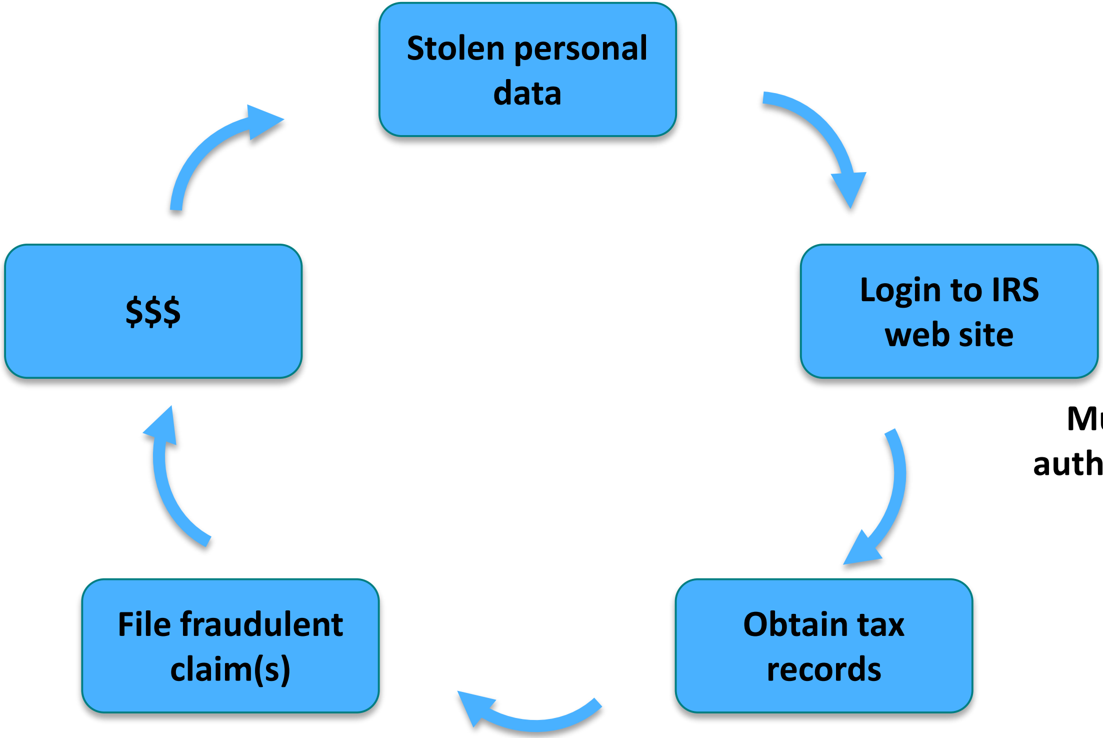
http://krebsonsecurity.com/2012/01/phishing-your-employees-101/

- Policy
- Procedure
- Process

Just When You Thought it Was Safe

http://www.nytimes.com/2015/05/27/business/breach-exposes-irs-tax-returns.html?_r=0

Some But Not Enough Security



Stolen personal data

Login to IRS web site

Obtain tax records

File fraudulent claim(s)

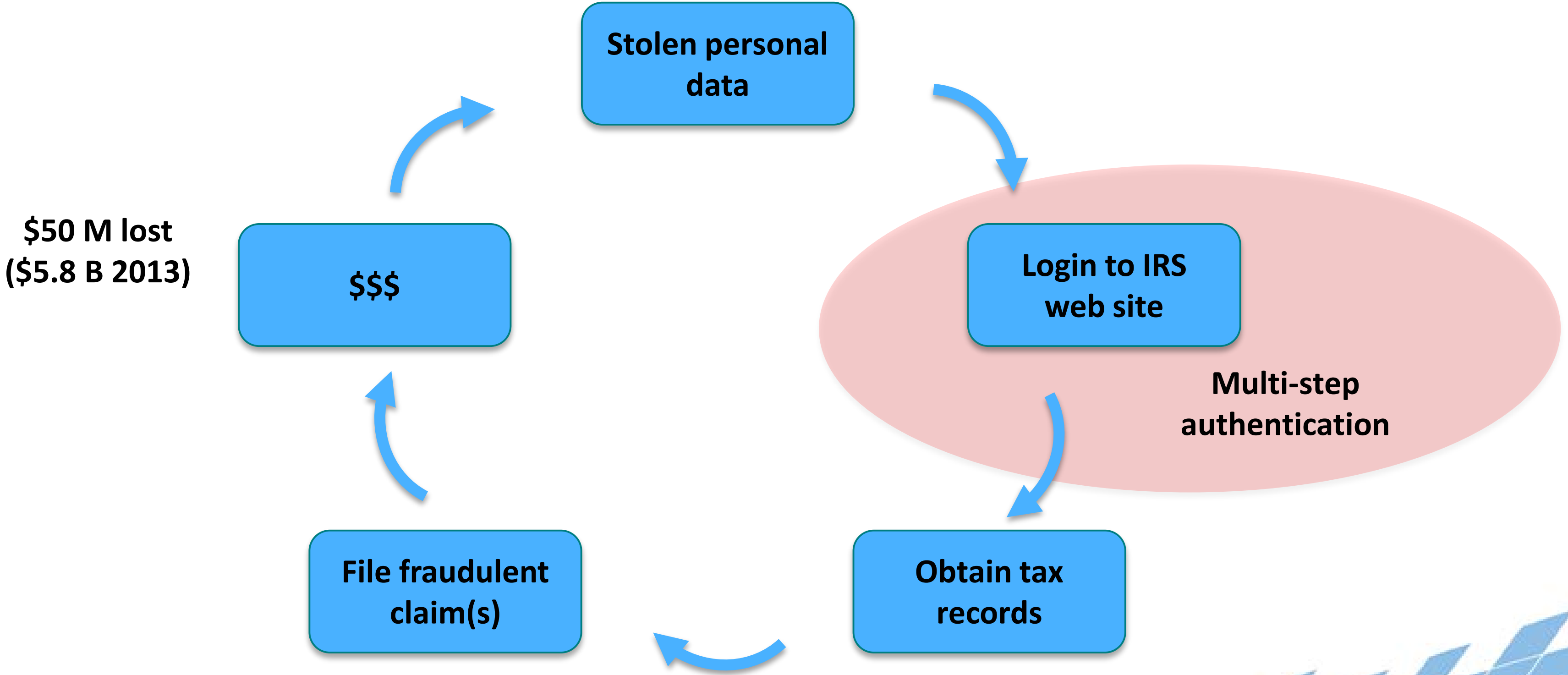
$$$

$50 M lost
($5.8 B 2013)

Multi-step
authentication

200,000 attempts
(Feb – May 2015)
100,000 records accessed

Some But Not Enough Security



Stolen personal data

Login to IRS web site

Multi-step authentication

Obtain tax records

File fraudulent claim(s)

$$$

$50 M lost
($5.8 B 2013)

200,000 attempts
(Feb – May 2015)
100,000 records accessed

Not a Good Summer for the US Government

“OPM director said stolen passwords for a federal contractor were used by hackers in the two cyber attacks targeting federal employee data.”

"It's really no surprise that the OPM breach was traced back to a compromised credential as this is the case in nearly 80% of the breaches we have seen, including Target and Anthem,"

Idan Tendler, head of Fortscale

http://krebsonsecurity.com/2015/06/catching-up-on-the-opm-breach/

Looking Forward

- ✓ Technology is only part of the solution
- ✓ Consider single vendor solutions but only if elements actually work together
- ✓ Remember your network extends beyond you
  - ✓ Remote employees, third party suppliers and contractors
- ✓ Your employees are the first line of defense – Equip and use them
- ✓ Never assume
  - ✓ You’re fully protected
  - ✓ The network hasn’t been breached