

# **COUNTERMEASURE**

## **IT Security Conference 2017**

If I Had a Million Dollars

Presented by:  
Olivier Henchiri

# Objective

---

- Discuss common challenges related to investing in IT security
- Present key factors for identifying IT security controls that offer the best value for your organization
- Share practical approaches and tools to support your strategy

# Challenges

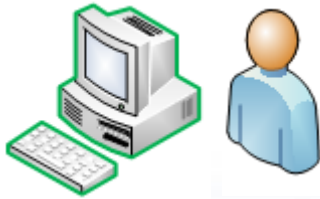
---

- Investments in IT security face:
  - Limited budgets
  - Competing priorities
  - Fast-changing technology landscape
  - Evolving threats
  - Reactive organizations

# Cyber Attack Scenario #1

---

Phishing email



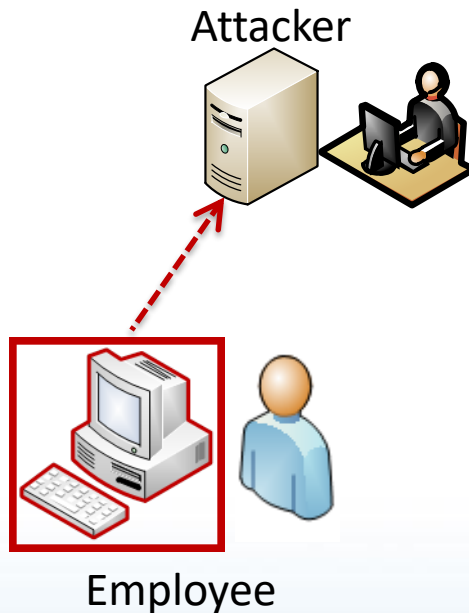
Employee

## Key Events:

- User receives phishing email
- Executes malicious file
- Compromises workstation

# Cyber Attack Scenario #1

---



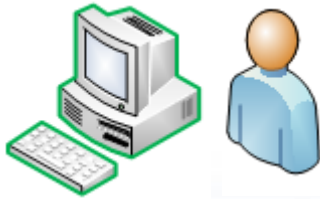
## Key Events:

- Undetected malware
- Exfiltration of data

# Cyber Attack Scenario #2

---

Spear phishing email



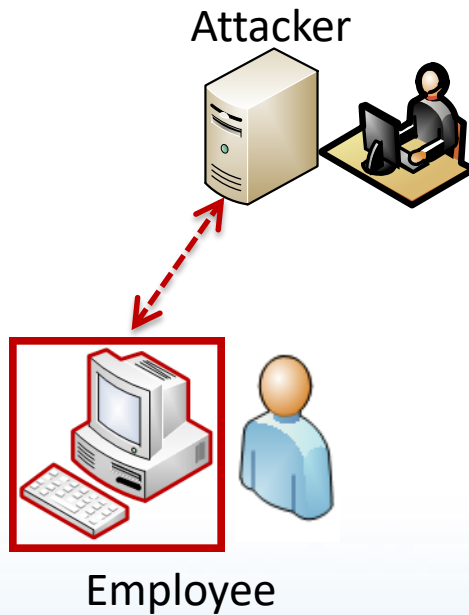
Employee

## Key Events:

- Receives spear phishing email
- Executes malicious file
- Compromises workstation

# Cyber Attack Scenario #2

---

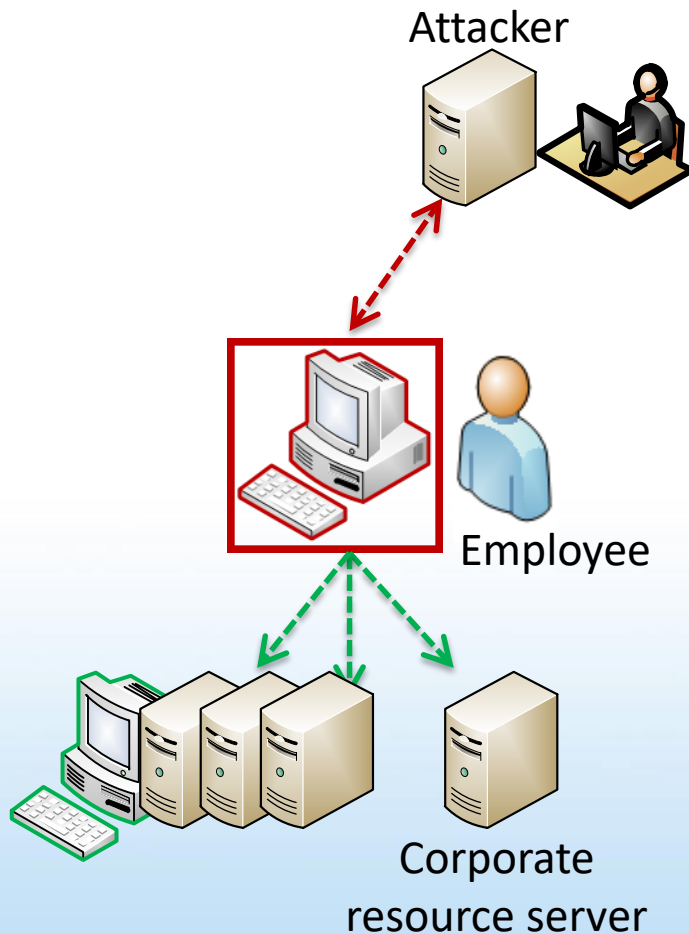


## Key Events:

- Connects with attacker
- Establishes Command & Control (C&C)

# Cyber Attack Scenario #2

---



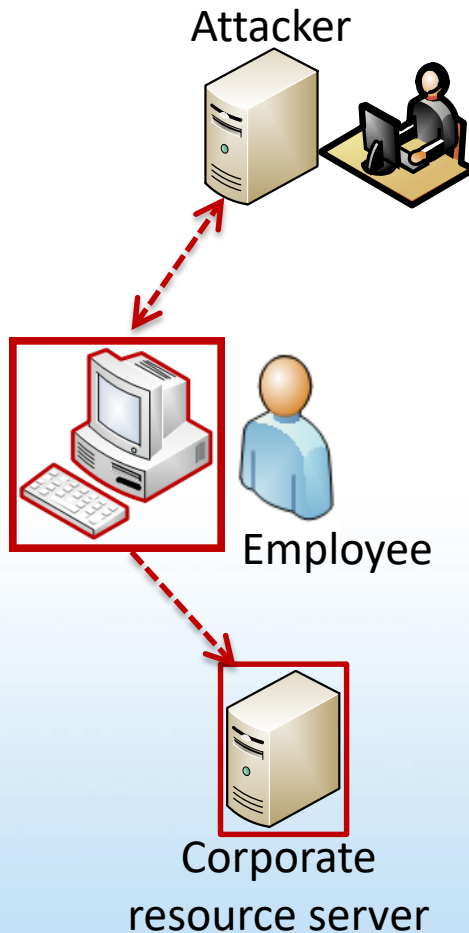
## Key Events:

- Conducts reconnaissance
- Identifies valuable assets



# Cyber Attack Scenario #2

---



## Key Events:

- Finds & exploits vulnerability
- Compromises internal asset

# Chimera® Ransomware



You are victim of the Chimera® malware. Your private files are encrypted and can not be restored without a special key file. Maybe some programs no longer function properly!

Please transfer Bitcoins to the the following address to get your unique key file.

**Address:**

**Amount: 0,93945085 Bitcoins**

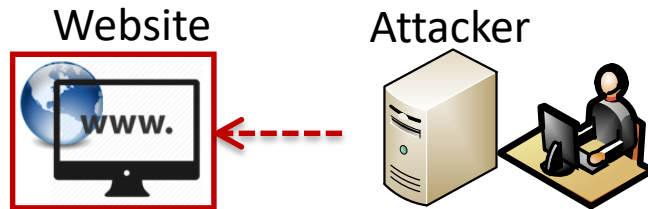
For the decryption programm and additional informations, please visit:

If you don't pay your private data, which include pictures and videos will be published on the internet in relation on your name.

Take advantage of our affiliate-program!  
More information in the source code of this file.

# Cyber Attack Scenario #3

---

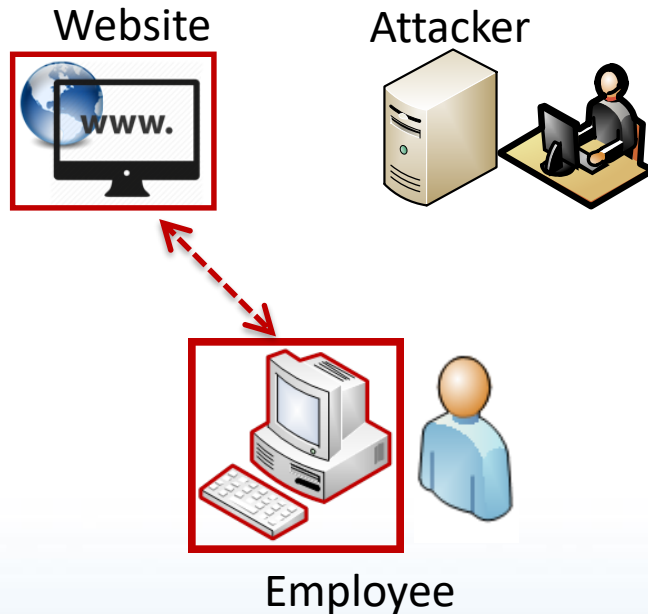


## Key Events:

- Attacker compromises legitimate website

# Cyber Attack Scenario #3

---

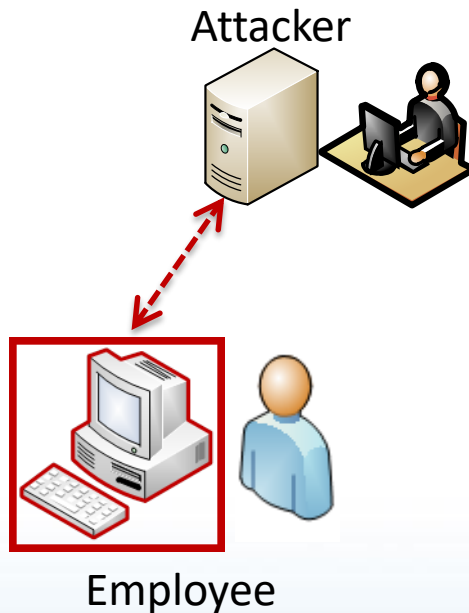


## Key Events:

- User visits website
- Website compromises workstation

# Cyber Attack Scenario #3

---

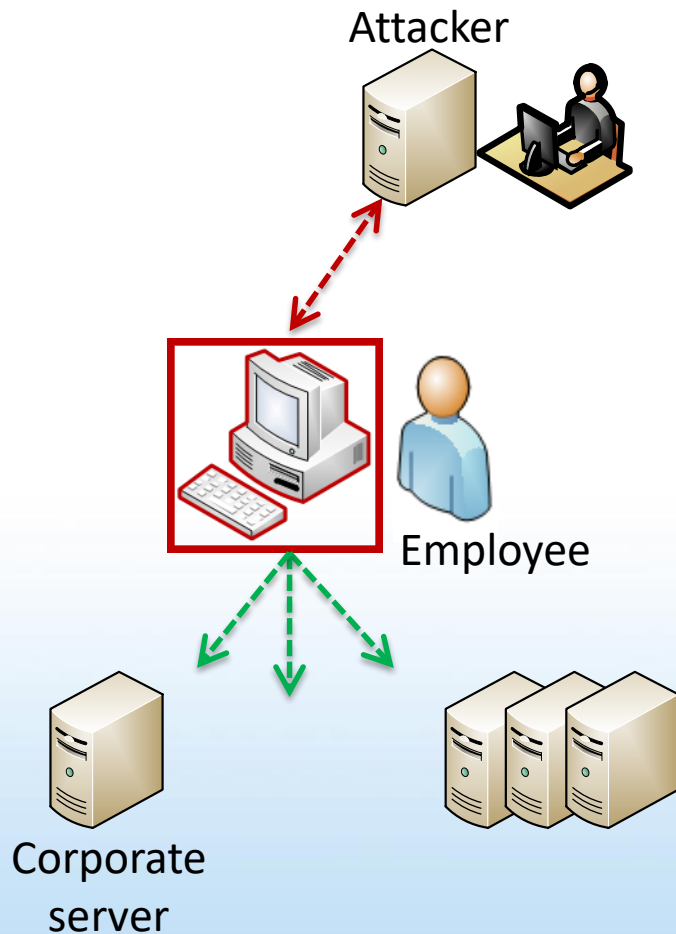


## Key Events:

- Connects with attacker
- Establishes Command & Control (C&C)

# Cyber Attack Scenario #3

---

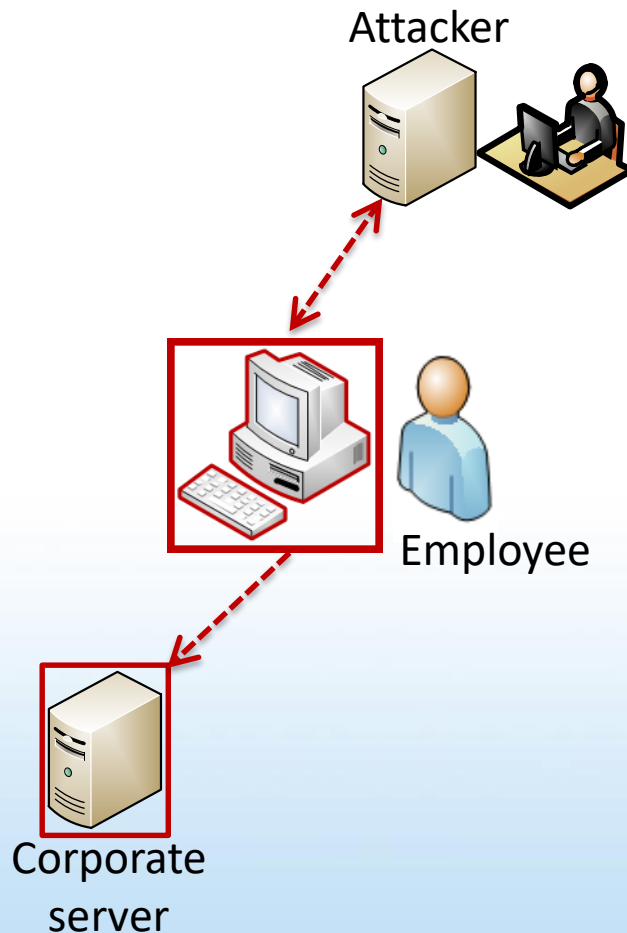


## Key Events:

- Conducts reconnaissance
- Identifies valuable assets

# Cyber Attack Scenario #3

---

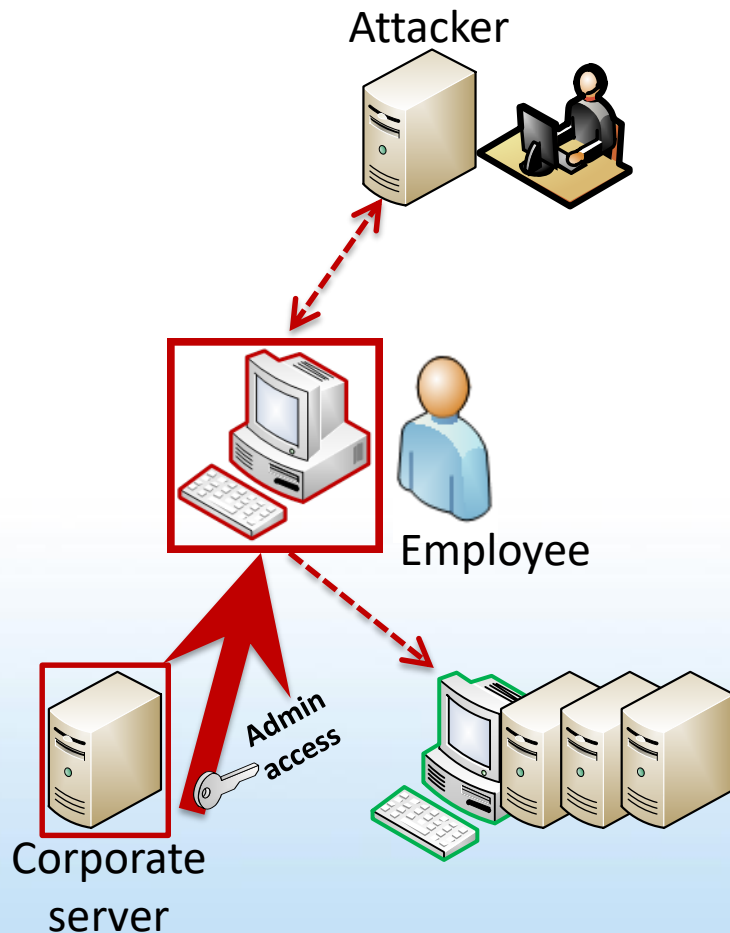


## Key Events:

- Finds & exploits vulnerability
- Compromises internal asset

# Cyber Attack Scenario #3

---



## Key Events:

- Steals admin credentials
- Uses it for lateral movement
- Establishes network persistence



# Lessons Learned

---

- Reactive approach
  - No single solution
  - Always one step behind
  - Fails to protect the organization
  - Does not identify priorities
  - May not yield the best value

# IT Security Needs

---

- Define your organization's IT security needs
  - Identify business activities
  - Determine security categories
  - Conduct threat assessments
  - Specify security control objectives
  
- ITSG-33 Annex 1
  - “Departmental IT Security Risk Management Activities”


# Residual Risk

---

**Asset Value x Threat x Vulnerability**





# Portable Data Storage Devices



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada



[Home](#) → [OPC News](#) → [News and announcements](#)

## Backgrounder

### Loss of portable hard drive containing personal information of student loan borrowers

**OTTAWA, March 25, 2014** — A portable hard drive containing the personal information of 583,000 student loan borrowers went missing in 2012 from Employment and Social Development Canada (ESDC), formerly Human Resources and Skills Development Canada. The hard drive also contained personal information about 250 [ESDC](#) employees. [ESDC](#) cannot say if the disappearance resulted from human error or malicious intent.

### What went wrong?

The Office of the Privacy Commissioner of Canada's investigation identified weaknesses related to four types of controls, which are the "pillars" of sound privacy management.

1. Physical controls
  - [ESDC](#) policy required that such portable storage devices be stored in a lockable filing cabinet when not in use. Our investigation established that the hard drive was often left unsecured for extended periods of time. Even when it was stored in a filing cabinet, the cabinet was in an open cubicle and often not locked.


# Travel Security

**The Telegraph**HOME | NEWS

News

UK | World | Politics | Science | Education | Health | Brexit | Royals

## Heathrow investigates after Queen's security details 'found on USB drive discovered lying in street'



Armed police officers patrol the new Terminal 5 at Heathrow Airport. CREDIT: GETTY

By **Mike Wright**  
29 OCTOBER 2017 • 10:15AM

**A** memory stick containing sensitive Heathrow security data, including the Queen's route to the airport, was reportedly found lying in the street.

A total of 76 files on the drive contained maps and restricted documents, reports the Sunday Mirror.

The USB stick, which was discovered by an unemployed man in north London, detailed the exact route the Queen takes to the airport and her security measures as well as those for cabinet ministers and foreign dignitaries, according to the newspaper.

It also reportedly contained other sensitive information such as a timetable of security patrols guarding against terror attacks and the types of ID needed for restricted areas.

# Availability

**CBCnews**

[Home](#) [Opinion](#) [World](#) [Canada](#) [Politics](#) [Business](#) [Health](#) [Entertainment](#) [Video](#)

## Latest Shared Services Canada outages disrupt border traffic

**Computer network designed to assure security at Canada-U.S. border crashes 200-plus times**

By Dean Beeby, CBC News | Posted: Nov 05, 2017 5:00 AM ET | Last Updated: Nov 05, 2017 5:00 AM ET

An internal briefing document says trucking has been disrupted at Canada-U.S. border points because of frequent computer crashes of a national security system since 2015. (Darryl Dick/Canadian Press)

80 shares

Facebook

Twitter

A border-security computer system has been crashing repeatedly, disrupting truck traffic into Canada, in the latest technical foul-up by Shared Services Canada, the beleaguered federal IT agency.

The so-called Advance Commercial Information (ACI) system, which requires all truckers to transmit digital information about their imports

# Data Holdings


**THE VERGE** TECH · SCIENCE · CULTURE · CARS · REVIEWS · LONGFORM · VIDEO

TECH CYBERSECURITY

## UK hospitals hit with massive ransomware attack

*Sixteen hospitals shut down as a result of the attack*

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT



A massive ransomware attack has shut down work at 16 hospitals across the United Kingdom. [According to The Guardian](#), the attack began at roughly 12:30PM local time, freezing systems and encrypting files. When employees tried to access the computers, they were presented with a demand for \$300 in bitcoin, a classic ransomware tactic.

The result has been a wave of canceled appointments and general disarray, as many hospitals are left unable to access basic medical records. At least one hospital has canceled all non-urgent operations as a result.

According to [a statement from the National Health Service](#), the culprit is a ransomware strain known as Wanna Decryptor (also known as WannaCry). While operations at the hospitals



# Authentication

## IT WORLD CANADA

CIO SECURITY MOBILE CLOUD RESEARCH EVENTS NEWS VIDEO BLOGS MORE



### Ashley Madison attack aided by credentials theft: Report



**Howard Solomon** @howarditwc

Published: August 24th, 2016

Poor administrator identity and access management controls were at the heart of last year's huge data breach at Avid Life Media Inc. (now called Ruby Corp.), the Canadian parent company of Ashley Madison and related global dating sites, that led to the release of personal and information of 36 million user accounts.

The lack of multi-factor authentication for controlling remote administrative access was described as a "significant concern" by the privacy commissioners of Canada and Australia [in a joint report issued Tuesday](#) into the breach.

It's an old but known problem: According to this year's [annual Verizon Data Breach Investigation report](#), 63 per cent of the 3,141 confirmed data breaches it investigated around the world last year involved leveraging weak, default or stolen passwords.



# Social Media

**theguardian**

home > world > US > americas > asia > australia > africa > middle east > cities > deve

## US Central Command Twitter account hacked to read 'I love you Isis'

Twitter avatar used by @CENTCOM was replaced with an image of a masked militant and the legends 'CyberCaliphate' and 'I love you Isis'



TWEETS	FOLLOWING	FOLLOWERS	FAVORITES
3,672	1,268	109K	30

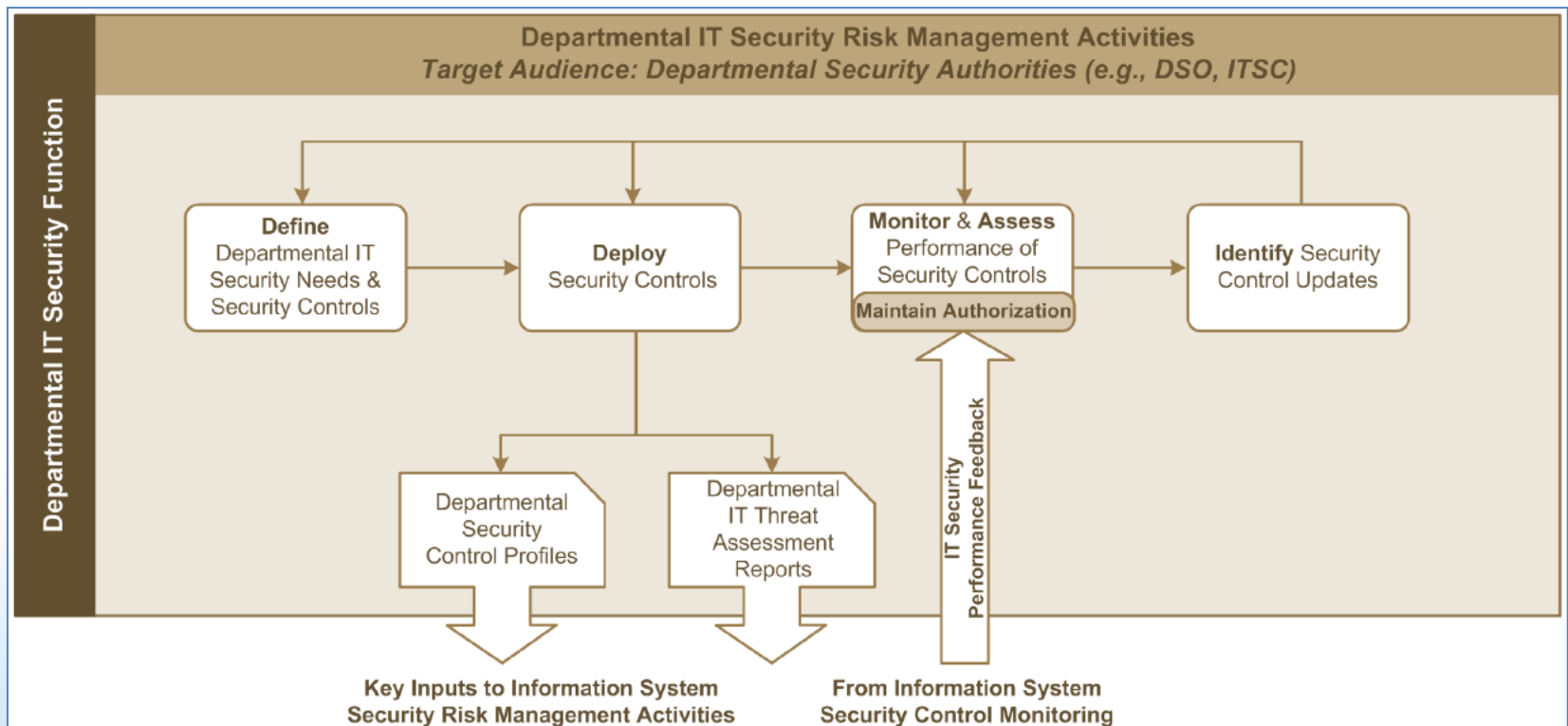
U.S. Central Command  
@CENTCOM

Central Command said it was aware of the apparent hack.

In an act of cyber vandalism that appeared more embarrassing than destructive, the Twitter and YouTube accounts for US military forces in the Middle East and South Asia were hacked by supporters of Islamic State militants on Monday.

# Formal Methodology

## ITSG-33 Annex 1



# Practical Inputs

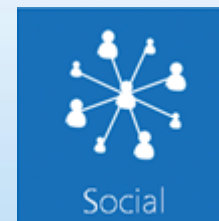
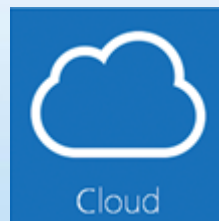
---

- Threat and risk assessments
- Departmental security plan
- Corporate risk profile
- Business continuity plan
- Audits
- Incident reports

# Technology Trends

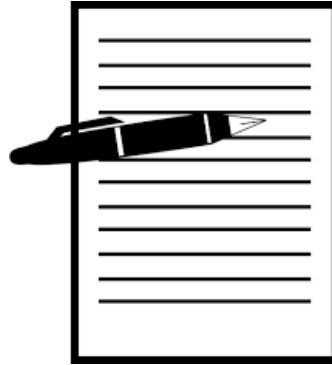
---

- Mobile devices
- Wireless Technologies
- BYOD
- Cloud services
- Social media
- Big Data
- The Internet of Things



# Risk Register

---



- Dedicated IT security risk register
  - Rated list of recommended controls
  - Class D cost estimates
  - Maintain year to year

# Supporting Tools

---

- CSE Top 10
- TBS IT policy implementation notices
- MAF
- Departmental security plan
- Corporate risk profile
- Departmental plan

# Questions?

