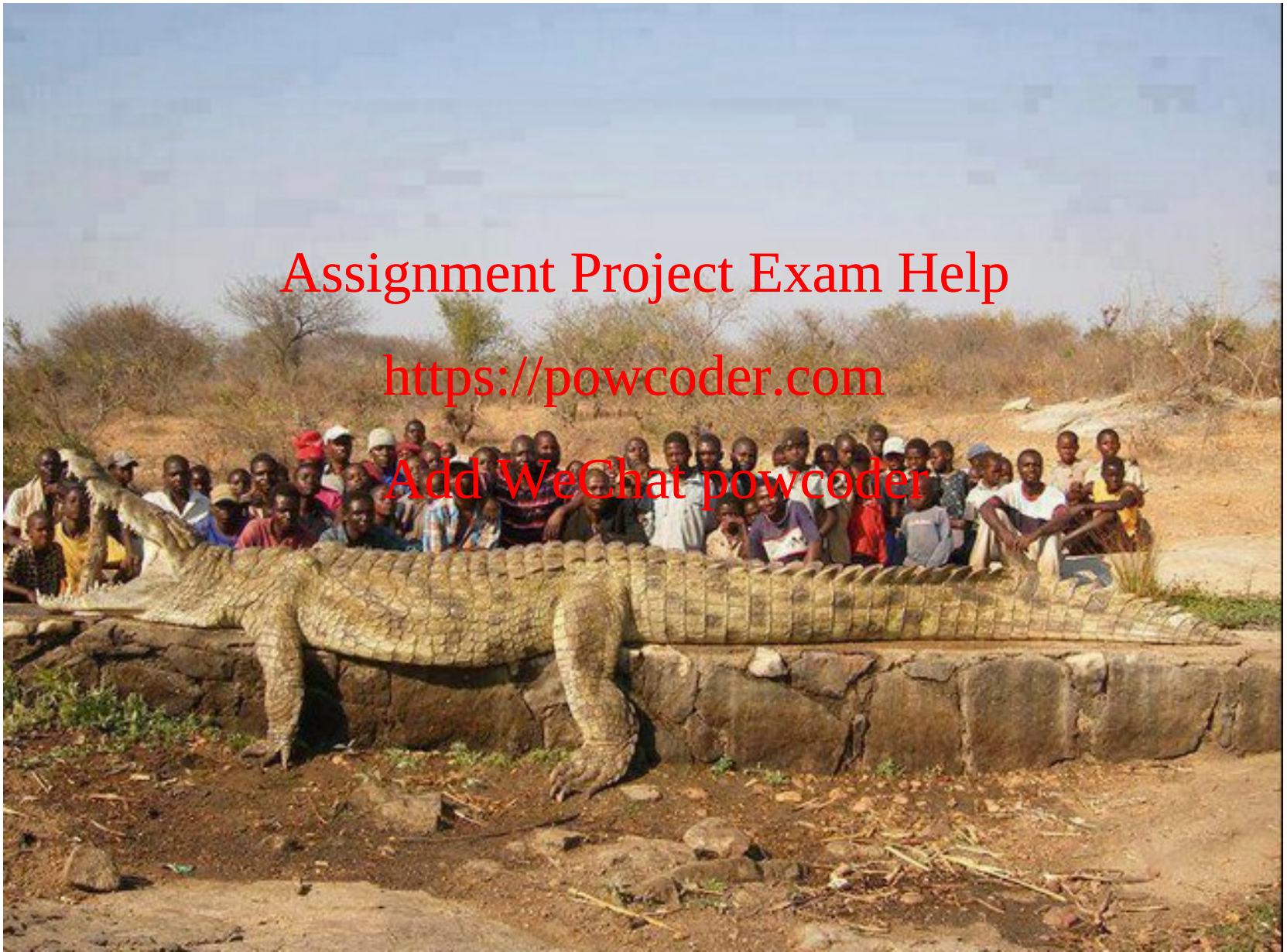
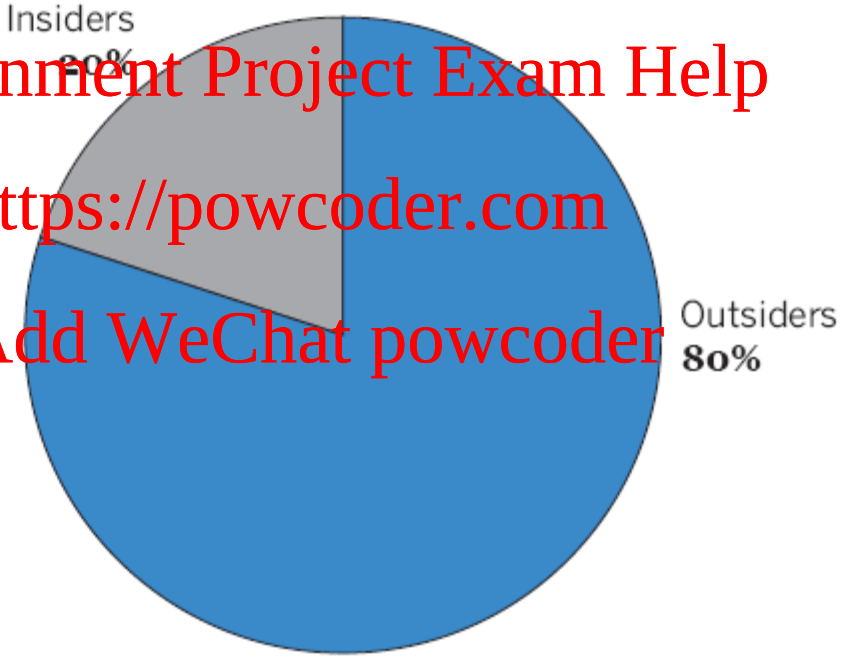
HUMAN-CENTRED SECURITY

Some People Think the danger is outside the Perimeter

How big is the threat?



Mean Percent of Electronic Crimes Caused by Outsiders vs. Insiders (base: among those experiencing electronic crimes)



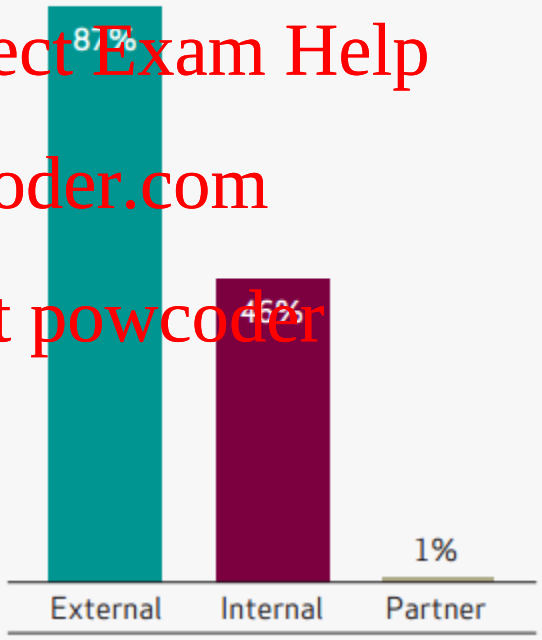
2005 Results (base: 554)

Verizon Study – Oct 2012

Table 1. Organizational size (number of employees) by number of threat types involving Intellectual Property theft

1 to 10	2
11 to 100	10
101 to 1,000	11
1,001 to 10,000	31
10,001 to 100,000	33
Over 100,000	14

Figure 1. Threat agents by percent of breaches involving Intellectual Property theft



Threat Actions

Figure 2. Threat action categories by percent of breaches involving Intellectual Property theft

CERT's Insider Threat Case Database

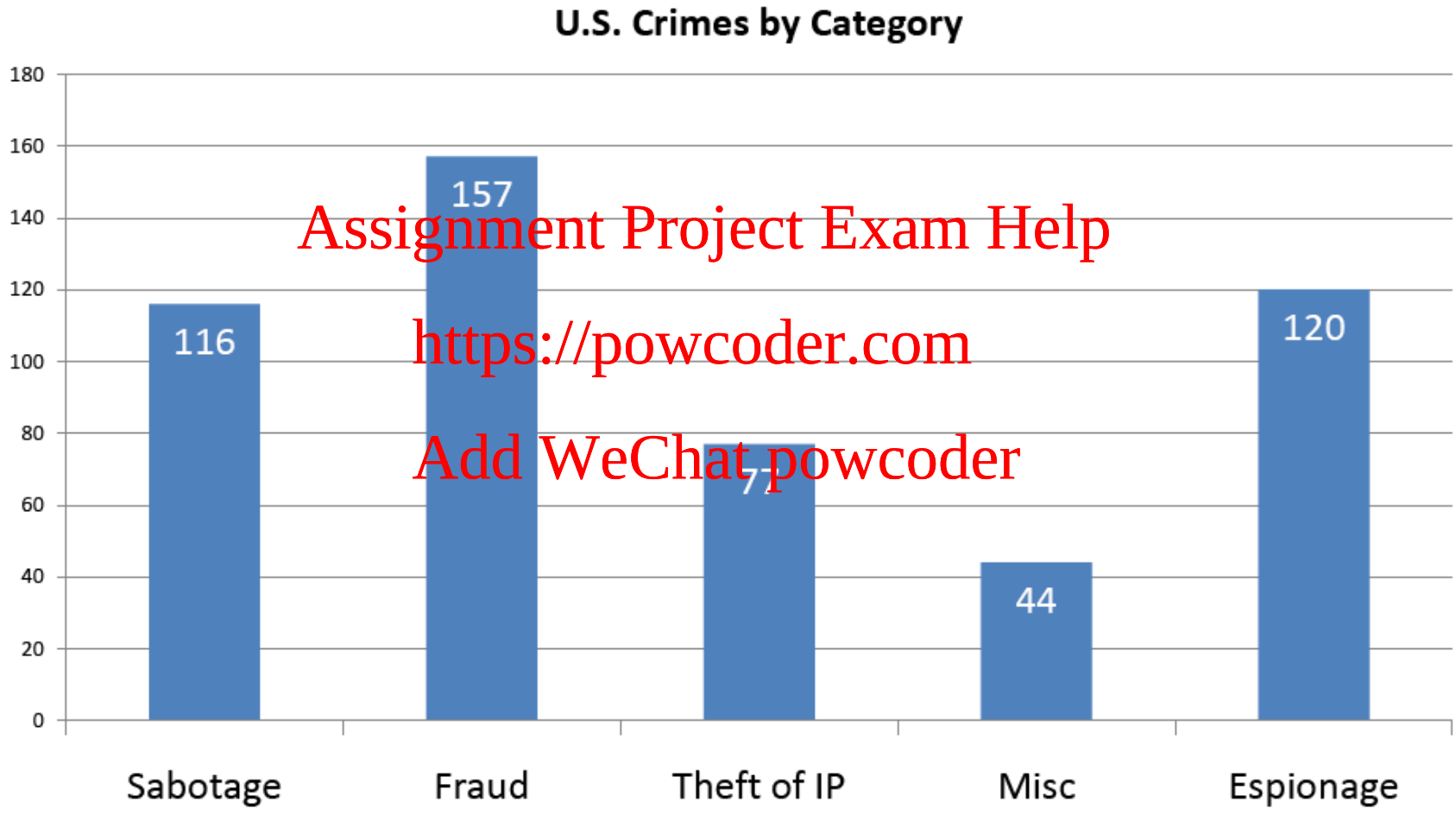
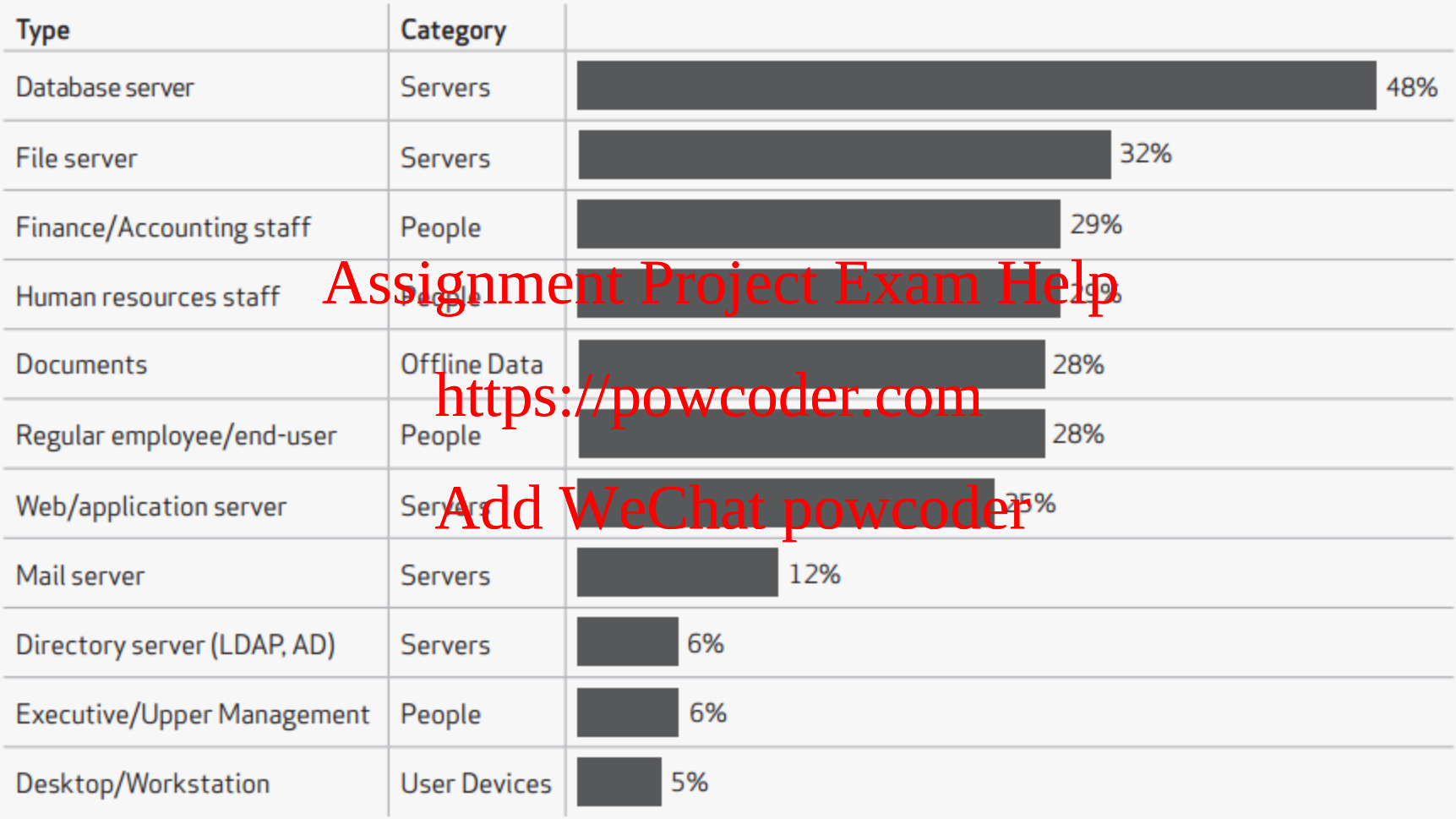


Table 2. Threat action varieties by percent of breaches involving Intellectual Property theft

Rank	Variety	Category	Breaches
1	Abuse of system access/privileges	Misuse	45%
2	Use of stolen login credentials	Hacking	34%
3	Pretexting (classic Social Engineering)	Social	32%
4	Solicitation/Bribery	Social	28%
5	Embezzlement, skimming, and related fraud	Misuse	28%
6	Exploitation of backdoor or command and control channel	Hacking	25%
7	Backdoor (allows remote access / control)	Hacking	24%
8	Keylogger/Form-grabber/Spyware (capture data from user activity)	Malware	22%
9	Send data to external site/entity	Malware	22%
10	System/network utilities (PsTools, Netcat)	Malware	22%
11	Brute force and dictionary attacks	Hacking	20%
12	SQL Injection	Hacking	20%

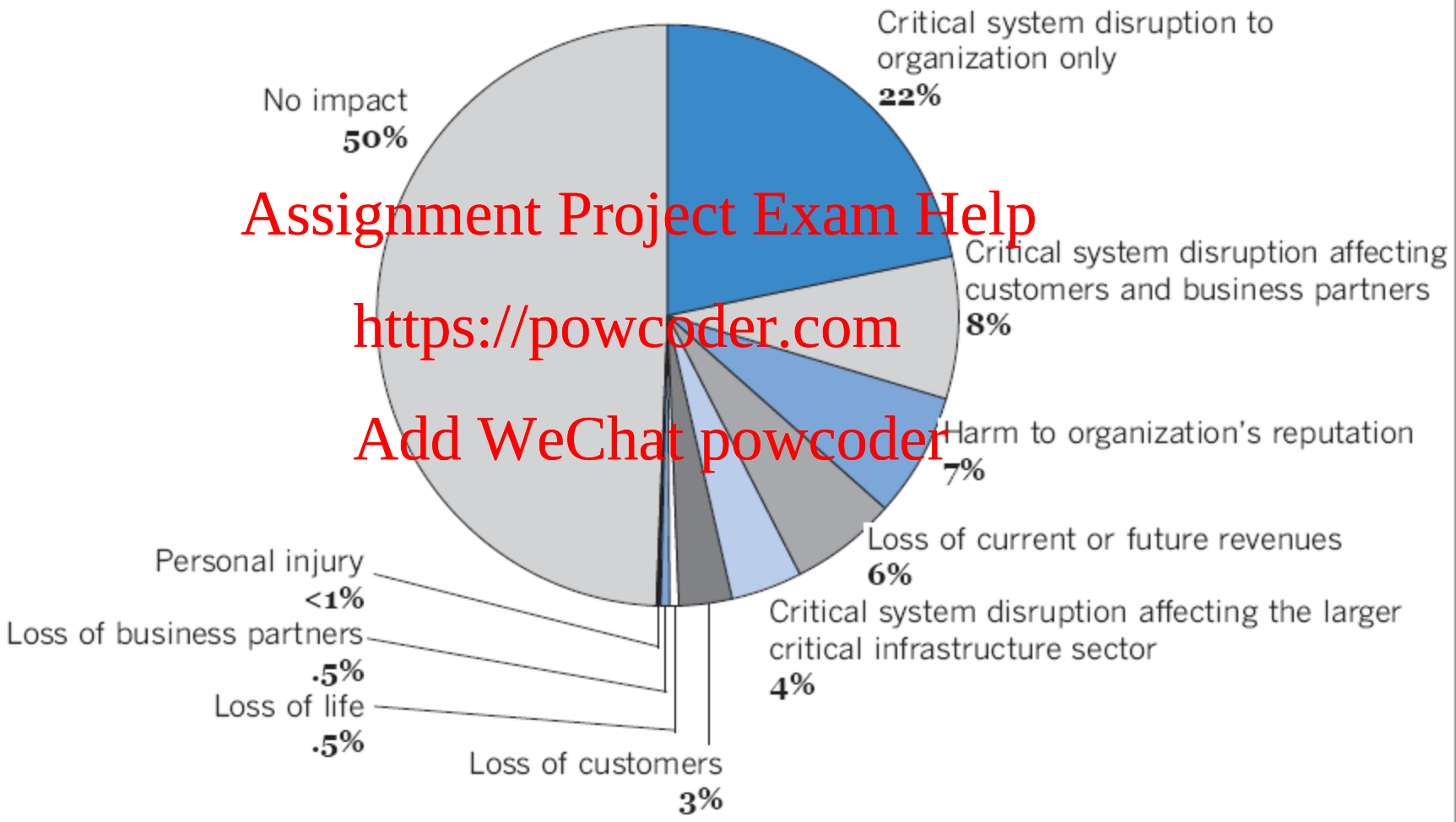
Figure 4. Compromised assets by percent of breaches involving Intellectual Property theft*



Type	Category	
Database server	Servers	48%
File server	Servers	32%
Finance/Accounting staff	People	29%
Human resources staff	People	29%
Documents	Offline Data	28%
Regular employee/end-user	People	28%
Web/application server	Servers	25%
Mail server	Servers	12%
Directory server (LDAP, AD)	Servers	6%
Executive/Upper Management	People	6%
Desktop/Workstation	User Devices	5%

*Assets involved in less than 1% of breaches are not shown

With respect to your organization, what is the most adverse consequence that has ever occurred from an insider network, data, or system intrusion?



2005 Results (base: 819)

Outsider Insider

Toyota says it was hacked by ex-IT contractor, sensitive information stolen

Join thousands of others, and sign up for Naked Security's newsletter

Don't show me this again

by Graham Cluley on August 29, 2017 | 0 Comments

FILED UNDER: Data loss, Featured, Law & order, Vulnerability

Toyota has accused an IT contractor that the car manufacturer fired just last week of breaking into its computer systems, and stealing sensitive information including trade secrets.

In a complaint filed at the US District Court in Lexington, Kentucky, the North American branch of the Toyota Motor company claimed that Ibrahimshah Shahulhameed illegally accessed one of its websites, after being dismissed from his contracting job on August 23rd.

Within hours of his dismissal, Shahulhameed is said to have logged into the toyotasupplier.com website without authorisation, and spent hours downloading proprietary plans for parts, designs and pricing information.

The website is used by Toyota's suppliers to exchange highly sensitive information with the company about current and future products.

Employee Context

Employee Context

- Permanent employees
  - initially vetted
  - above suspicion
  - subsequent checks
- Temporary employees
  - not subjected to the same checks
  - less likely to exhibit loyalty
  - privileged access to resources
  - Example: Zhangyi Liu
- Former employees
  - backdoor access
  - stockpile resources (passwords etc)
  - seek vengeance
  - Example: Donald Burleson

Focus

- **Focus on all employees?**

Focus

- **Focus on all employees?**
- **Critical Information Technology Insiders (CITIs).**
  - **they design, maintain and/or manage critical information systems.**

Misuse Categories

Misuse Categories

- **Intentional**
  - self-interest and resources.
  - malicious intent.
  - waste resources (e.g. shopping, self-promotion).
- **Accidental**
  - employees circumvent policies to complete tasks (e.g. sticky note with password).
  - employees may leak sensitive information through actions (e.g. social networks, 'Reply All' instead of 'Reply').
- **Ignorance**
  - lack training and awareness (e.g. device not encrypted).
  - unattended equipment and observed in public.
  - disposing or taking resources when leaving job.

Insiders – Defined by Access

- **ASPECTS OF INSIDERS:**
- **Are on the inside, with access privileges**
- **They are trusted**
- **Access privileges accrue over time**
- **Aware of policies, procedures & technology**
- **Know where the valuable data is and how to access it**

As of 20th July 2011,

534,978,831 records

have been breached in USA since 2005,

of which 32,106,583 records

breached

by Insiders alone

Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

party, malware and spyware.

- [ ] **Payment Card Fraud (CARD)** - Fraud involving debit and credit cards that is not accomplished via hacking. For example, skimming devices at point-of-service terminals.
- [x] **Insider (INSD)** - Someone with legitimate access intentionally breaches information - such as an employee or contractor.
- [ ] **Physical loss (PHYS)** - Lost, discarded or stolen non-electronic records, such as paper documents
- [ ] **Portable device (PORT)** - Lost, discarded or stolen laptop, PDA, smartphone, portable memory device, CD, hard drive, data tape etc.
- [ ] **Stationary device (STAT)** - Lost, discarded or stolen stationary electronic device such as a computer or server not designed for mobility.
- [ ] **Unknown or other (UNKN)**

- [x] EDU - Educational Institutions
- [x] GOV - Government and Military
- [x] MED - Healthcare - Medical Providers
- [x] NGO - Nonprofit Organizations

- [x] 2005
- [x] 2006
- [x] 2007
- [x] 2008
- [x] 2009
- [x] 2010
- [x] 2011
- [x] 2012
- [x] 2013
- [x] 2014

GO!

Select features, then click GO.

New Search

Help Guide

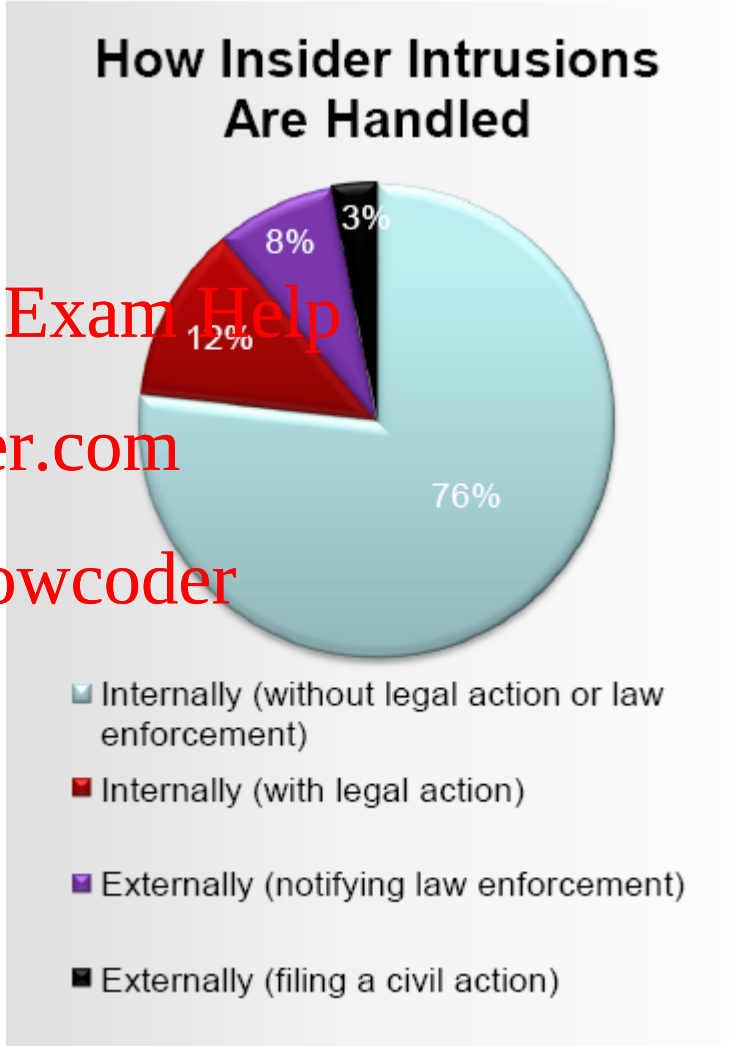
Return to Chronology main page.

Breach Subtotal

Breaches currently displayed:
Breach Types: INSD
Organization Types: BSO, BSF, BSR, EDU, GOV, MED, NGO
Years: 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014
32,682,969 Records in our database from.
535 Breaches made public fitting this criteria

Damage

- Financial
- Reputation
- Business Operations
- Harm to specific individuals
- Availability of data compromised



IRS

- Claude Carpenter
- Contractor.
- Accessed servers and inserted malicious code to cause havoc.
- Aim was to get him back to solve problems.
- Hid tracks by turning off logs, removing code to ensure he would not be uncovered.

Traffic Nightmare LA

- Two employees in the middle of a labour dispute sabotaged all the traffic lights
- One actually implemented the system
- Access had been removed!

How?

- They used their supervisor's access (he had shared his credentials)
- Murillo allegedly accessed the system and found a way to lock other managers from fixing the changes. Prosecutors reported it took four days to repair the signals.

TRUE STORY:

Emergency services are forced to rely on manual address lookups for 911 calls on Friday night...

Employee sabotages the system and steals all backup tapes

National Security at Risk by Insiders

- Terrorist Watch List was tampered with by employee in government agency outside the U.S.
  - Wife's name was added to the list three years earlier so she could not return after leaving the country to visit family.

Immigration officer fired after putting wife on list of terrorists to stop her flying home

By STEVE DOUGHTY FOR THE DAILY MAIL
UPDATED: 18:11, 30 January 2011

An immigration officer inserted himself of his wife by adding her name to a list of terrorist suspects.

He used his access to security databases to include his wife on a watch list of people banned from boarding flights into Britain because their presence in the country is 'not conducive to the public good'.

As a result the woman was unable for three years to return from Pakistan after travelling to the county to visit family.

The tampering went undetected until the immigration officer was selected for promotion and his wife name was found on the suspects' list during a vetting inquiry.

The Home Office confirmed today that the officer has been sacked for gross misconduct.

The incident is likely to raise new questions over levels of efficiency in the

Immigration officer fired after putting wife on list of terrorists to stop her flying home

By STEVE DOUGHTY FOR THE DAILY MAIL
UPDATED: 18:11, 30 January 2011

Employment context

An immigration officer inserted himself of his wife by adding her name to a list of terrorist suspects.

He used his access to security databases to include his wife on a watch list of people banned from boarding flights into Britain because their presence in the country is 'not conducive to the public good'.

As a result the woman was unable for three years to return from Pakistan after travelling to the county to visit family.

The tampering went undetected until the immigration officer was selected for promotion and his wife name was found on the suspects' list during a vetting inquiry.

The Home Office confirmed today that the officer has been sacked for gross misconduct.

The incident is likely to raise new questions over levels of efficiency in the

Products Shipped with Embedded Malware

- Malware embedded in product forces shutdown after random number of power cycles
  - Contract programmer of 30 years devised the scheme so he could start a side repair business

A Picture is Worth a Thousand Words…

- Company's trade secrets photographed and emailed outside the U.S.
  - Two engineers servicing the company's equipment used mobile phone to take pictures for use in their own contract with Chinese firm.

Employee sabotage grounded 2,000 Chicago flights, authorities allege

Complaint details how paramedics followed trail of blood past gas can, two knives and a lighter to find employee Brian Howard

Associated Press in Chicago
theguardian.com, Saturday 27 September 2014 15.32 BST

Jump to comments (25)

Passengers fill available seats as they wait to travel after flights were delayed or cancelled at O'Hare International Airport in Chicago. Photograph: Tannen

Howard worked for the FAA contractor that supplies and maintains communications systems at air traffic facilities, said Jessica Cigich, a spokeswoman for Professional Aviation Safety Specialists, the union that represents FAA technicians. Howard was recently told he was being transferred to Hawaii, according to the complaint filed in US district court in Chicago.

Encrypting the Information

- A System Administrator learns that she is to be downsized
- She decides to encrypt important parts of the database and hold it hostage
- She will decrypt it in return for substantial "Severance Pay" and promise of no prosecution
- The organization decides to pay without consulting with proper authorities and they are precluded from pursuing charges

Changing the Configuration

- An engineer is on probation after a series of confrontations with co-workers
- After he has been reprimanded without pay pending resolution of the situation, it is discovered that the network configuration has been changed denying the organization's clients the services they have been promised
- Only the engineer holds the privileges to change them. Unfortunately he is not interested in helping out

Mail Flood

- A major Aerospace company recently fired an employee who caused its e-mail system to crash for six hours after sending thousands of other employees a personal e-mail that requested an electronic receipt
- They lost hundreds of hours of productivity

Deleting Company Files

- July 1996, Omega
- A recently demoted employee created a software "time bomb" that affected the network files
  - Deleted the company's "most critical software programs"
- Result:
  - Caused a loss of over $10 million
  - 80 people lost jobs

True Story - Revenge

A company's mobile devices were suddenly disabled for almost 1000 employees, grinding sales and delivery operations to a halt for several days …

Logic bomb went off three months to the day after a demoted system architect's retaliatory resignation.

True Story - Revenge

- Employee loaded a virus
- Cost R20m and affected 700 stores
- He had a grudge against the group for outsourcing its information technology maintenance and support work
- 80% of the details for stores in South Africa were deleted, customer sales had to be entered manually and hard drives were damaged.

True Story – Financial Gain

A company sues a former programmer found selling a competing product at a tradeshow….

Investigators found copies of the company's source code on his home computer that was stolen on his last day of work at the company

True Story – Financial Gain

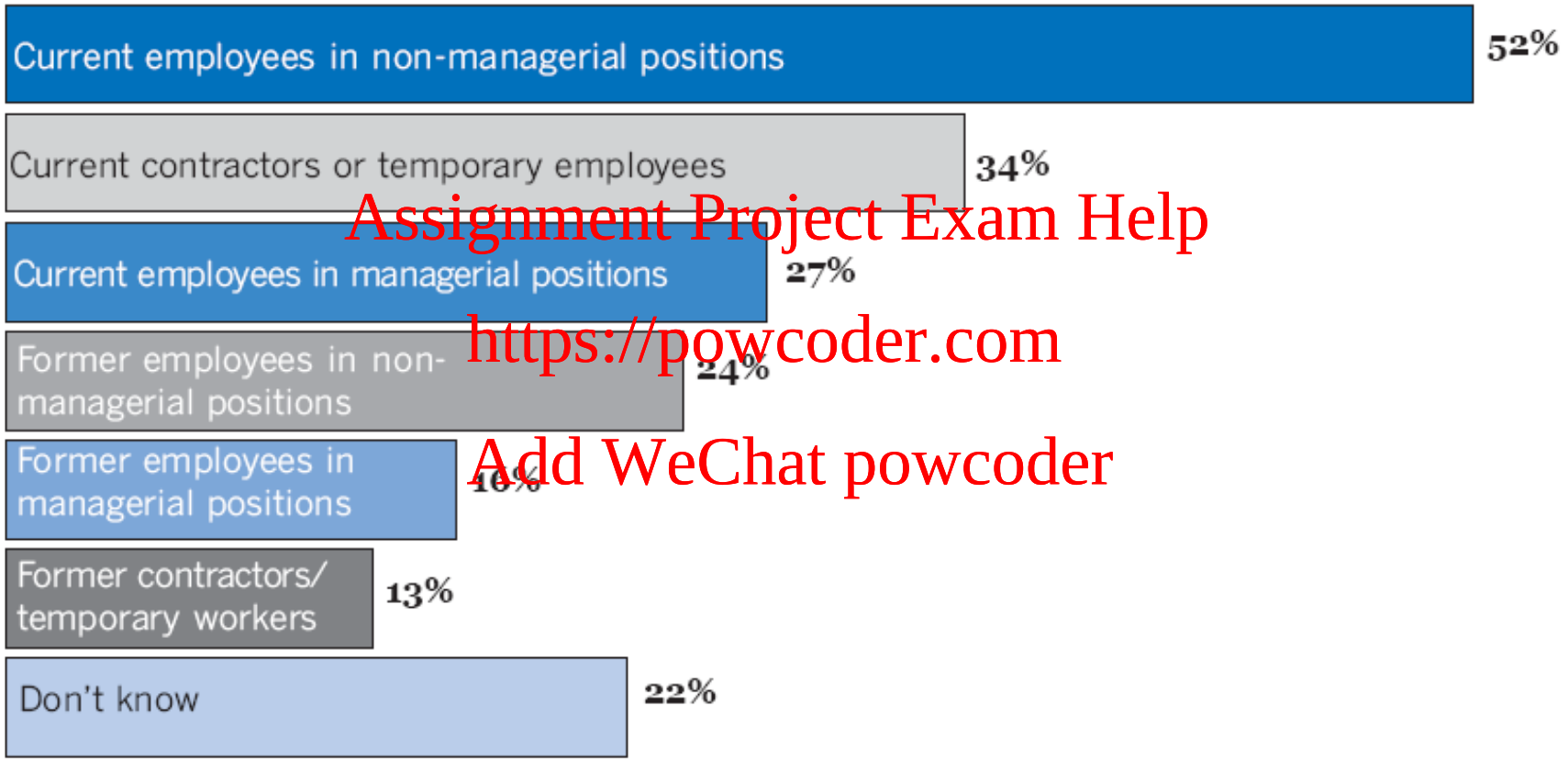
A financial organization's routine audit discovers a $90,000 discrepancy in one of their software engineer's personal loan accounts…

The employee modified critical source code to siphon off money to cover fraudulent personal loans he had created.

Who Are They?

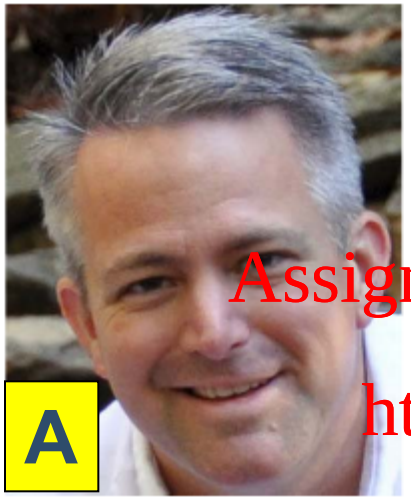
- Gender – mostly males
- Locus of Control – fatalists
- Attribution style – failure is due to external factors
- Core self-evaluations – similar to self-esteem
- Integrity – people who are agreeable, conscientious, stable, reliable less likely to do this
- Neuroticism – extent to which they experience anger, anxiety, fear, hostility
  - Neurotics feel people are too demanding, distant and threatening

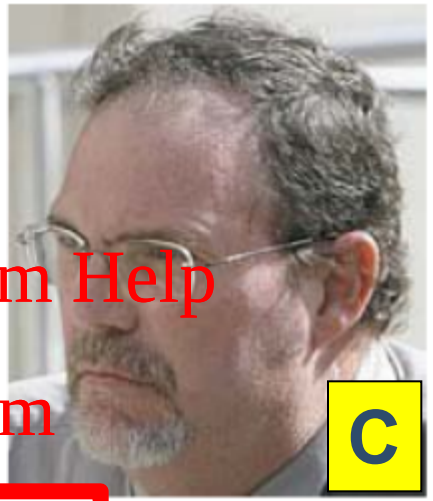
Please indicate all sources of insider intrusions in 2004 (base: those experiencing insider intrusions).

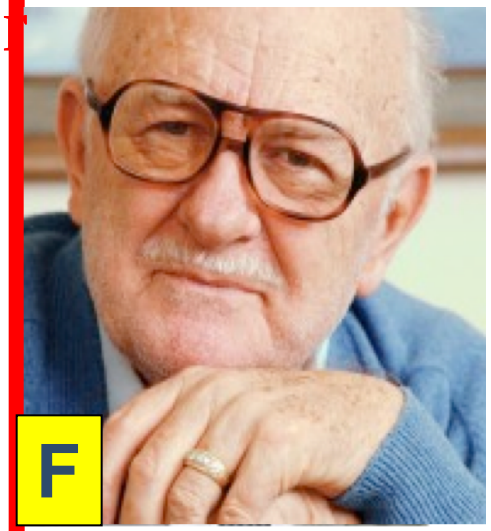


2005 Results (base: 214)

SPOT THE INSIDER…..





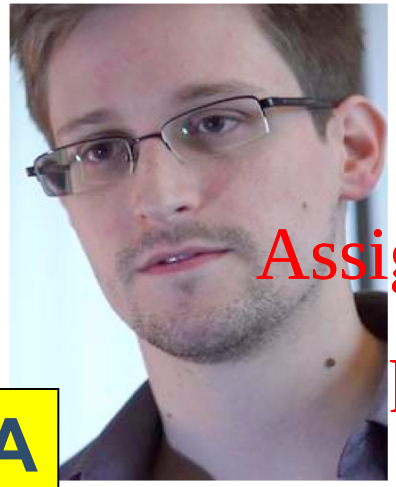


Terry Child, Convicted IT Administrator

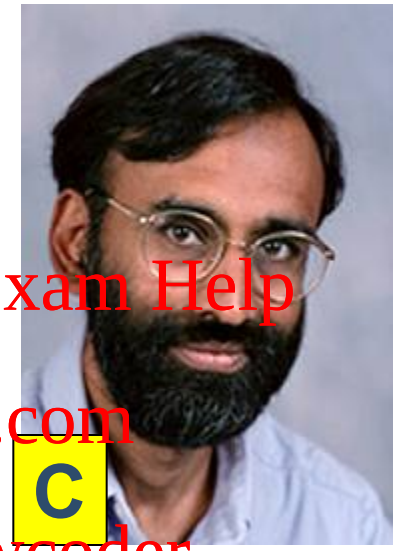
Terry Childs Case – San Francisco Net

- Terry Child: Responsible for creating and managing the City of San Francisco's FiberWAN network
- On July 9, 2008, told over a hostile conference call with the HR Dept., his boss and a police officer, that he was being reassigned and not working anymore on FiberWAN Network and is to hand over the passwords
- Hands over bogus passwords and reluctant to give the right passwords
- His Justification: nobody in the room was qualified to have admin access to the network
- In Prison for 7 years and bond of US$ 5 million
- Jury found him a nice guy, protective of his work, like many IT people, possibly a little paranoid.
- Didn't have a good management to keep him in check. Allowed free rein, which allowed engineering decisions over the years that made things worse and worse, and locked people out of possibly getting into this network

Spot the Threat


A


B


C


D


E


F

Ed Snowden

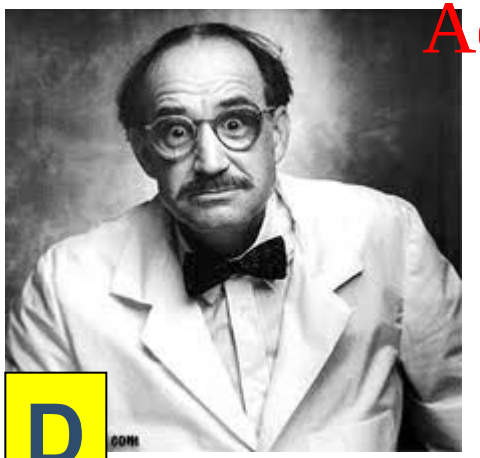
Edward Snowden statement: 'It was the right thing to do and I have no regrets'

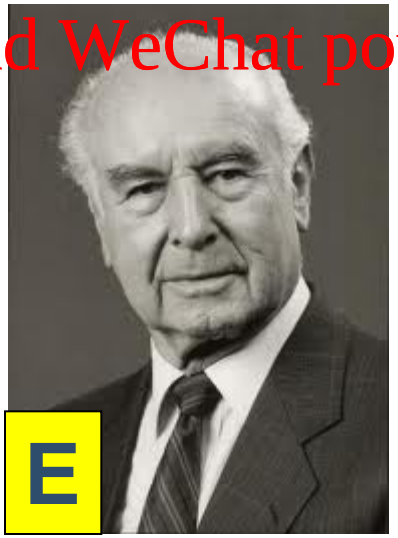
Full transcript of the statement made by Edward Snowden, in which he accepts all offers of asylum he has been given

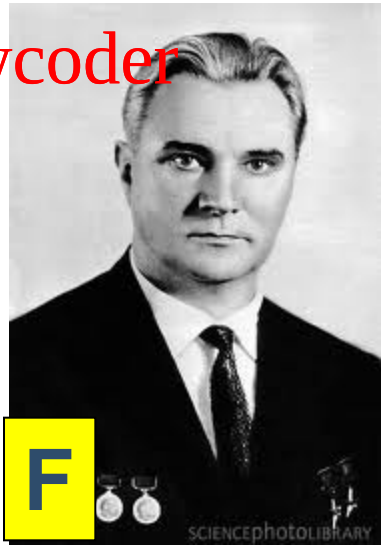
- Get the latest on Edward Snowden asylum developments

guardian.co.uk, Friday 12 July 2013 16.15 BST

Spot the Insider







Aldrich Ames - Money

- Sold info to the Soviet Union for $5m
- Disclosed over 100 covert operations
- Betrayed 30 double agents (10 executed)
- Crippled the CIA's activities for some years
- He did not use technology

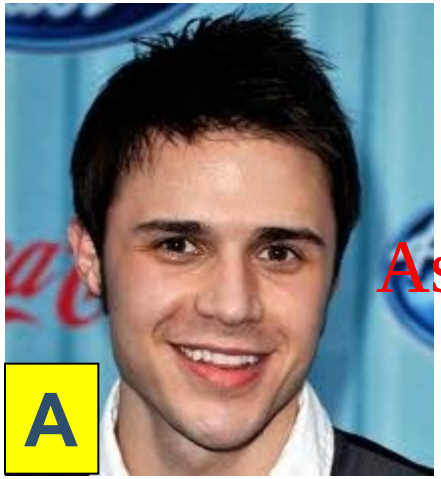
Robert Hanssen - Money

- Spied for the Soviets for 22 years
- Got $1.4m
- Even the Soviets didn’t know who he was
- Disclosed 1000s of secrets
- Accessed everything via his default access rights

Money

- Gary Min was a research scientist at DuPont
- Downloaded 16700 pdf documents ($400 m)
- Gave it to his new employer
- Most had nothing to do with his research
- 15 times more downloads than other users
- Only caught when he announced he was leaving and they started looking at the usage logs

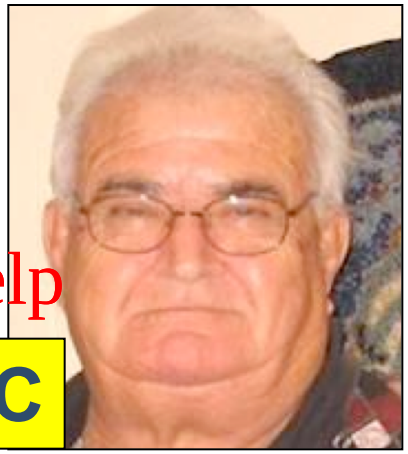
Spot the Insider



Bradley Manning

- US Soldier
- Provided info to WikiLeaks
- Transferred classified data onto his personal computer
- Arrested on May 26, 2010
- On March 1, 2011, an additional 22 charges were preferred, including wrongfully obtaining classified material for the purpose of posting it on the Internet, knowing that the information would be accessed by the enemy; the illegal transmission of defense information; fraud; and aiding the enemy.

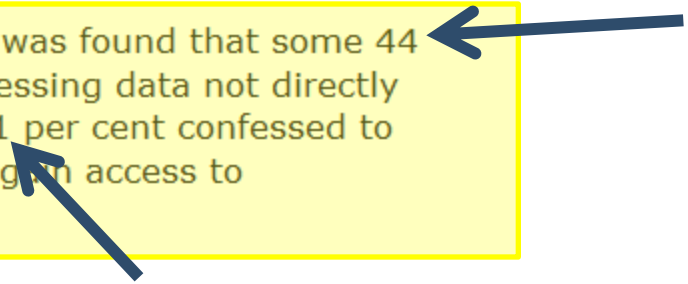
Spot the Insider



UBS PaineWebber (Roger Duronio)

- Sentenced to 97 months
- took down as many as 2,000 servers around the country in UBS PaineWebber offices.
- This meant that the company was unable to make trades for up to several *weeks* in some offices
- The company reported a cost of $3.1 million to recover from the attacks
- He had a criminal record!

In a recent survey by Cyber Ark, it was found that some 44 per cent of IT staff admitted to accessing data not directly related to their role, and another 31 per cent confessed to using admin passwords in order to gain access to confidential or sensitive data.



If that were not worrying enough for the average enterprise, it gets worse when you take into account that such insiders are often the very people most familiar with and therefore best placed to exploit network security controls.

"Associated with this insider threat is the need for organisations to implement comprehensive activity monitoring," advised Cyber Ark's Mark Fullbrook.

"Go beyond access control and privileges enforcement, and actually record and track the precise actions that were performed on which assets and by whom," Fullbrook suggested.

"Do that, and the enterprise should be able to integrate operational data and security analysis, providing a complete overview of their systems. Overall, if businesses are to mitigate the insider threat, they must look to invest in appropriate technology that ensures information is stored securely." Businesses also need systems that log and monitor all privileged identities and activities, Fullbrook concluded.

Majority of Employees Plan to Steal Company Data

Wednesday, November 24, 2010

Contributed By:
Headlines

A new study based in the UK reveals an alarming statistic: The majority of workers plan on stealing company data if and when they leave their current positions.

The survey of 1000 white collar employees conducted by Imperva shows that more than two-thirds are willing to take everything from client and customer records to the intellectual property of their employer.

Employees surveyed indicate they believe they have some sort of right to the data in question.

> *"It seems most employees have no deliberate intention to cause the company any damage. Rather, this survey indicates that most individuals leaving their jobs suddenly believe that they had rightful ownership to that data just by virtue of their corporate tenure,"* says Imperva CTO Amichai Shulman.

The study also revealed that 85% have confidential company information on their home computers or personal mobile devices, 75% admit to having client records, and 27% to having sensitive intellectual data.

Also revealed in the study was that at least half of the employees had accessed data they were not cleared to peruse, and three-quarters stated that the data access control mechanisms in place were easy to bypass.

- **2/3 would steal data if fired**
- **85% have confidential info at home**
- **75% have client records**
- **½ have accessed data they had no business accessing**
- **¾ said they could easily do this**

http://www.infoworld.com/d/security/many-employees-would-sell-corporate-information-study-finds-168110

JULY 26, 2011

Many employees would sell corporate information, study finds

A high percentage in Britain would be willing to steal corporate data and sell it for profit, as would some Americans and Australians

By Joan Goodchild | CSO

A survey of more than 3,400 employees in the United States, Great Britain, and Australia finds corporate loyalty be damned. Your company's data may be on its way out the door when certain employees resign or get laid off.

The research, conducted by Harris Interactive for security firm SailPoint, found a significant number of employees polled admitted to misusing using company data; a significant percentage in Britain said they would be comfortable selling proprietary and sensitive information for profit.

[Prevent corporate data leaks with Roger Grimes' "Data Loss Prevention Deep Dive" PDF expert guide, only from InfoWorld. | Stay up to date on the latest security developments with InfoWorld's Security Central newsletter.]

[Also see: The three types of insider threat]

Among the findings:

- Of those polled, 22 percent of US, 29 percent of Australian and 48 percent of British employees who have access to their employer's or client's private data indicated they would feel comfortable doing something with that data, regardless if that access was intentional or accidental.
- Many said they would forward electronic files to a non-employee, with 10 percent of Americans, 12 percent of Australians, and 27 percent of British employees indicating they would do so.
- Nine percent of Americans, 8 percent of Australians, and 24 percent of Britons admitted they would copy electronic data and files to take with them when they leave a company.

News

50% Job leavers steal confidential company data

16 July 2012

New details from Iron Mountain show the extent to which employees leaving employment will take confidential company data with them when they go.

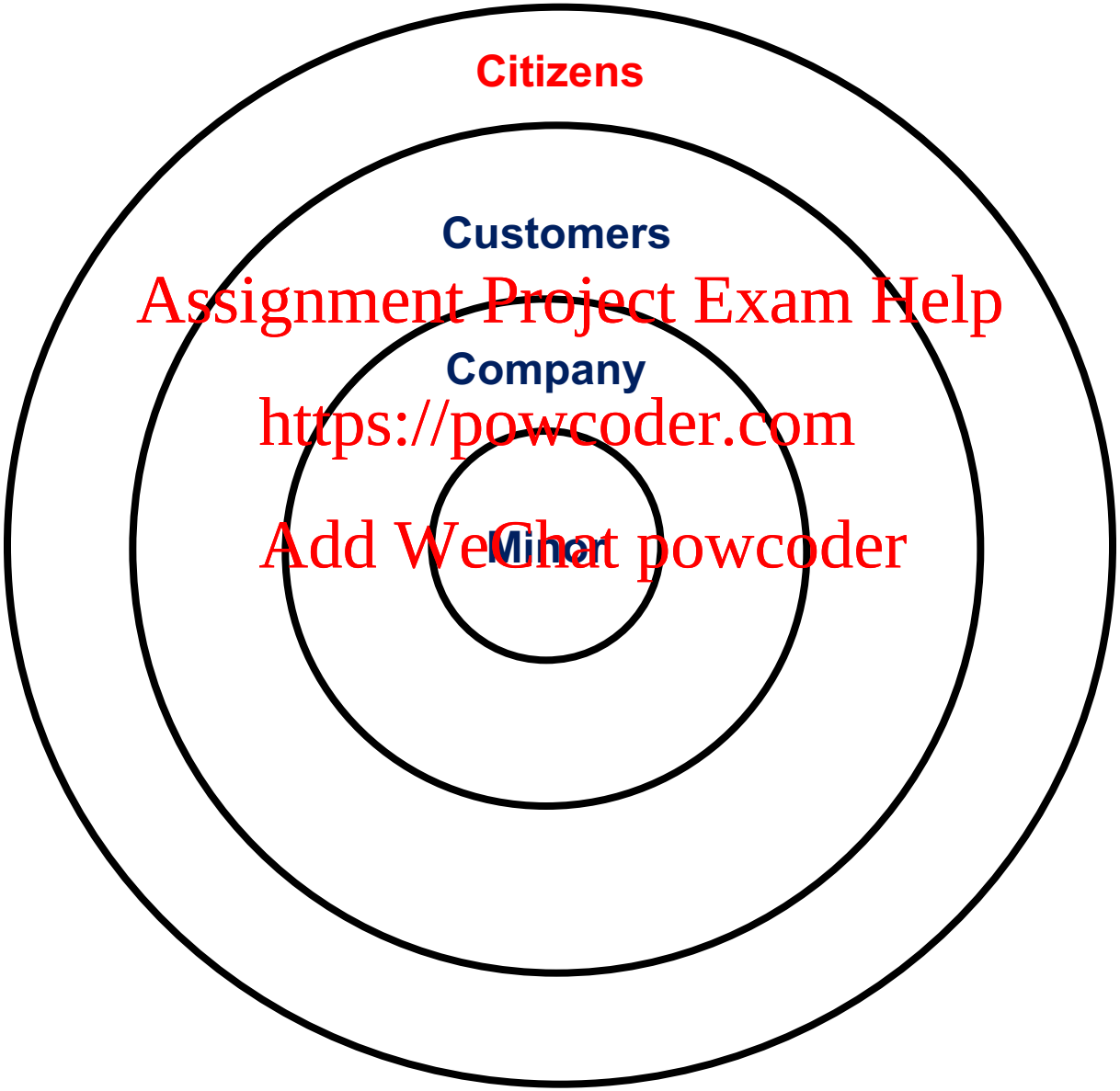
Iron Mountain surveyed 2000 French, German, British and Spanish office workers across all business sectors. They wanted to learn staff attitudes to company data when either moving on to a different job – or getting fired. The clear implication is that workers have a feeling of personal ownership when they are involved with the collection of that data.

Across Europe, more than half of office workers (51%) will take data with them when the switch jobs. It's slightly less in the UK at 44%. The main reason is not malice, but a belief that they have a right to the data they helped create, and a belief that it will help in any future job.

It's not just databases. Of those who do take information, 46% walk off with presentations, 21% with company proposals, 18% with strategic plans, and another 18% with product/service roadmaps – all of which, says Iron Mountain, represents highly sensitive and valuable information that is critical to a company's competitive advantage, brand reputation and customer trust.

"As businesses across Europe rush to tighten up their data protection policies in advance of new EU legislation," comments senior vice president Patrick Keddy, "it is extremely worrying to see that employees are leaving jobs with highly sensitive information." The problem is that the standard company security model is based on stopping electronic

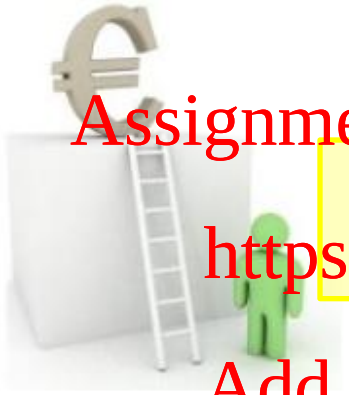
Circle of Damage



http://www.mobile-financial.com/node/14446/The-risk-profile-for-mobile-operators

The risk-profile for mobile operators

Hannes van Rensburg,
Date Posted: Sunday, July 10, 2011



Online banking in South Africa is much more secure because of the use of SMS to deliver one time passwords (OTP) to banking customers. Unfortunately, even this practice can be manipulated by criminals to intercept passwords. This was recently highlighted when it was reported that a Vodacom employee colluded with criminals to intercept the OTP's sent to customers. In the process fraud of R2.4 million (about $340 000) was committed. (Read **here**). The immediate question is if Vodacom is liable in any way for this damage and the answer is quite clearly: no.

The commercials and infrastructure that supports existing telecommunication services (the delivery of voice and data products), were never designed to cater for the additional liability of financial services. Many examples exist where banks have been held liable for fraud perpetrated on their networks (Read for instance **here**). Banks have to implement systems to cater for this, they have to price their products accordingly and take out insurance to achieve this. The question is if Mobile Operators understand these implications and if they are able (and willing) to act accordingly.

In the meantime, consumers have to be made aware that the protection that they may expect from utilising telecommunication infrastructure to secure their banking , are not as rigorous as they may think. This is demonstrated by a resent post on the Internet Security Awareness Portal (Read **here**).

http://mybroadband.co.za/news/cellular/8779-vodacom-at-centre-of-banking-sms-scam.html

Vodacom at centre of banking SMS scam

Rudolph Muller | July 13, 2009 | No comments | Tweet 0 | Recommend

Vodacom subscribers scammed out of R 2.4 million; cellular provider dodges questions about safety of SMS banking

Rudolph Muller

Rudolph Muller is the editor at MyBroadband and covers telecoms and broadband news. Rudolph comes from an academic background, but left the University of...

FOLLOW | Full Profile | E-mail

The Citizen recently revealed how a Vodacom employee, who was part of an SMS banking fraud syndicate, helped to scam banking clients out of R 2.4 million by diverting SMS notifications.

According to The Citizen all the victims of this scam were Vodacom subscribers whose "security chain between the bank and the online user has been breached."

This security breach raises serious questions about the safety of SMS banking. SMSs are used by various financial institutions as a secure method of communication, but this incident highlighted the vulnerability of using an SMS based system.

Security problems inside Vodacom – both in the form of a rogue employee and systems allowing such an employee to freely commit fraud – are a cause of concern amoung current Vodacom clients.

Vodacom said that it is unfortunate that a Vodacom staff member, in conjunction with an online banking syndicate, was able to commit fraud. "Vodacom has implemented additional security measures, to ensure that this type of fraud does not happen again," said Dot Field, Chief Communications Officer of the Vodacom Group.

Field added that Vodacom is working closely with the SAPS and SABRIC (South African Banking Risk Information Centre), and that the relevant employee is in SAPS custody and a criminal charge has been brought against the employee.

Vodacom however dodged questions about whether SMS banking is safe and did not provide any details about the measures it took to avoid the future occurrence of this type of scam.

Vodacom did warn that "due to the immediacy of online banking, consumers are reminded to keep their online banking details secure from any third party". This advice is however unlikely to put Vodacom subscribers'

Check your marital status

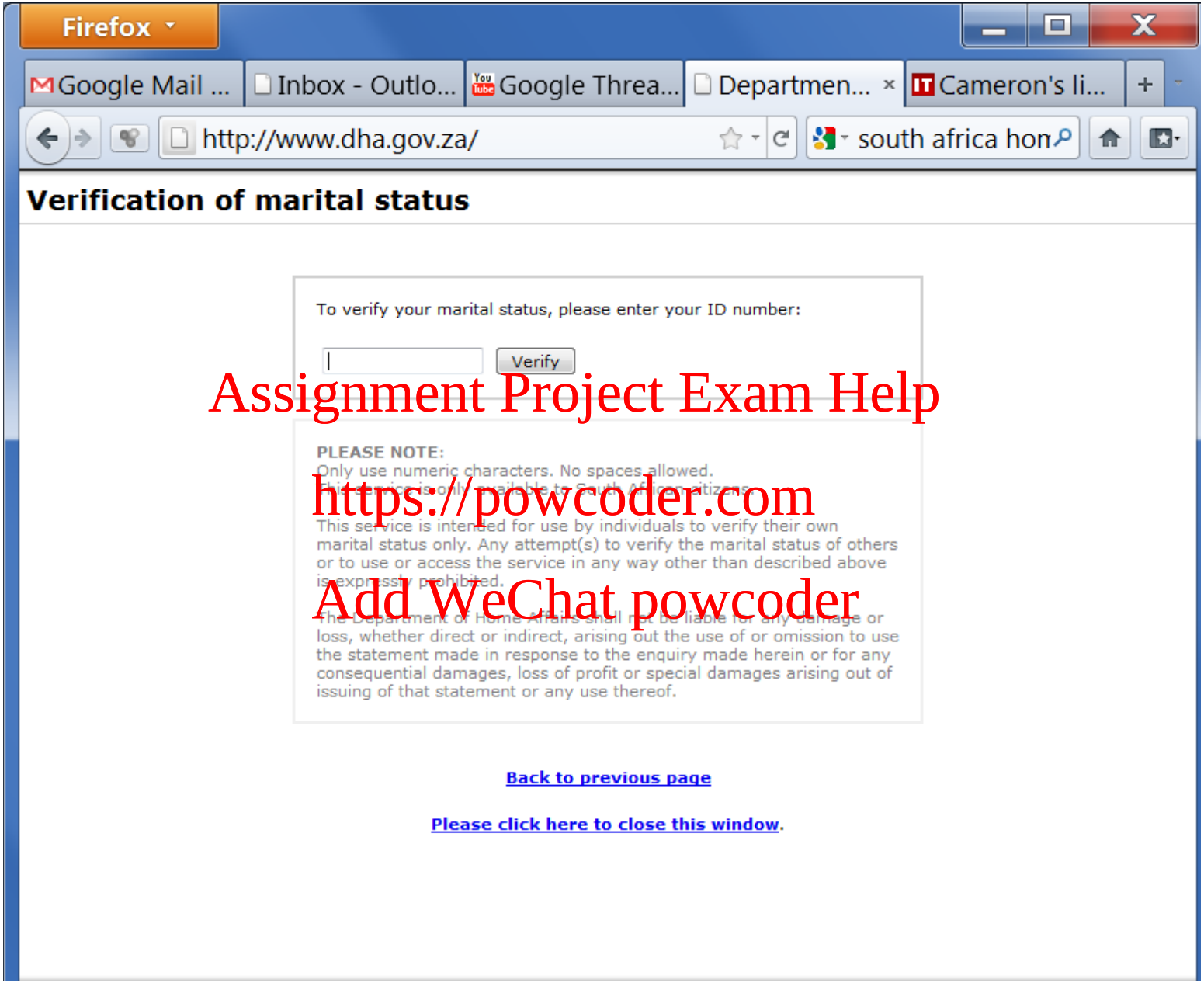
2004-08-04 10:27

Pretoria - South African women were urged on Tuesday to check that their marital status was reflected correctly on the records of the home affairs department.

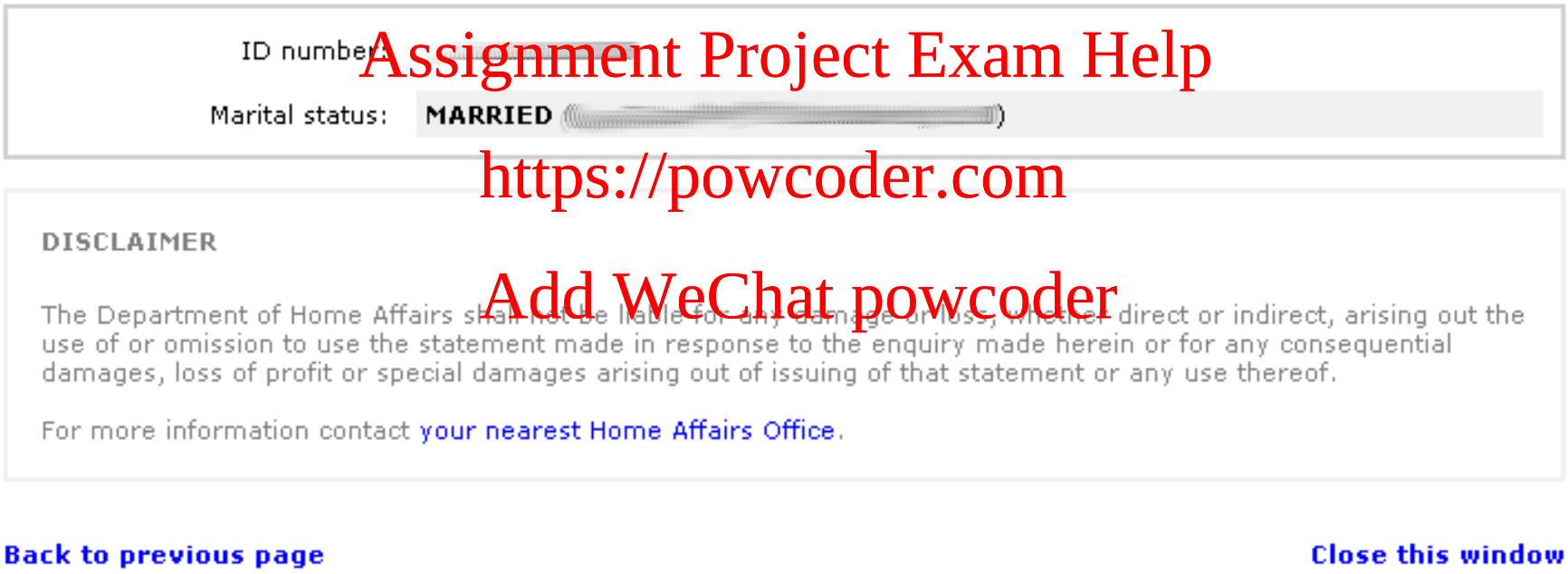
Home Affairs Minister Nosiviwe Mapisa-Nqakula launched a special "Check Your Status" campaign in KwaMhlanga, Mpumalanga, partly in a bid to curb the problem of women being married to foreigners without their knowledge.

Check Your Marital Status

DESCRIPTION:	The Department of Home Affairs has launched a new online marriage verification service as part of the Check Your Marital Status Campaign. The service has been made available to assist in preventing and uncovering instances where South Africans have been unknowingly married to foreigners. The foreign spouses use the marriage to get residence and work permits in South Africa. By 18 August 2004, the Campaign had uncovered 200 fraudulent marriages in South Africa. The Department has promised to nullify resident permits, work permits and citizenship of people who have benefited from fraudulent marriages.
INSTRUCTIONS:	If you are a South African citizen, you can check your marital status by logging onto the Department of Home Affairs website and submitting your ID number. You can also visit your local Home Affairs office to check your status or you can query the status via SMS. Send an SMS to **32551** and the message of the SMS should be as follows: • For your ID book application status: type **ID** then the ID number (eg **ID** 5001010050080). • For your passport application status: type the letter **P** and then the ID number (eg **P** 5001010050080). • For your marital status: type the letter **M** and then the ID number (eg **M** 5001010050080). • For your ID status (deceased or alive): type the letter **L** and then the ID number (eg **L** 5001010050080). You will receive the status directly to your cellphone via SMS.
PROVIDED AT:	These facility categories: • Home Affairs Offices



It worked!



26 July 2011 Last updated at 14:36

Woman invented four kids for £90,000 tax claim

A tax office worker who hijacked a woman's identity and invented four children to fraudulently claim £90,000 in benefits has been jailed.

Emily Barrass worked as a call centre advisor at a Dundee tax office

Emily Barrass, a call centre adviser at tax offices in Dundee, began claiming a stranger's benefits after moving into her former home in Arbroath.

She added two children to Susan Lindsay's claim and two to another woman's claim before she was caught.

Barrass, 39, pleaded guilty to the charges and was jailed for two years.

Dundee Sheriff Court heard she began working at Her Majesty's Revenue and Customs (HMRC) office in Dundee in March 2004 and moved into Miss Lindsay's home a year later.

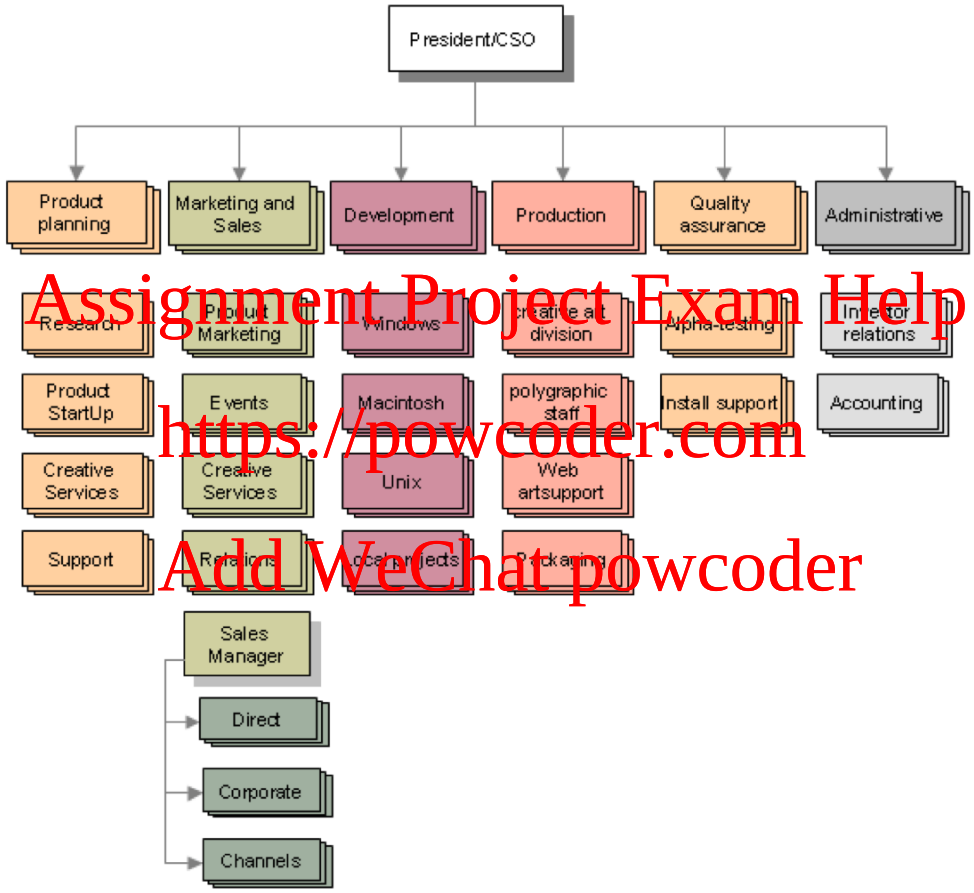
Miss Lindsay, who was unknown to Barrass, had a live claim for tax credits which were being paid into her bank account.

False call report

Reality

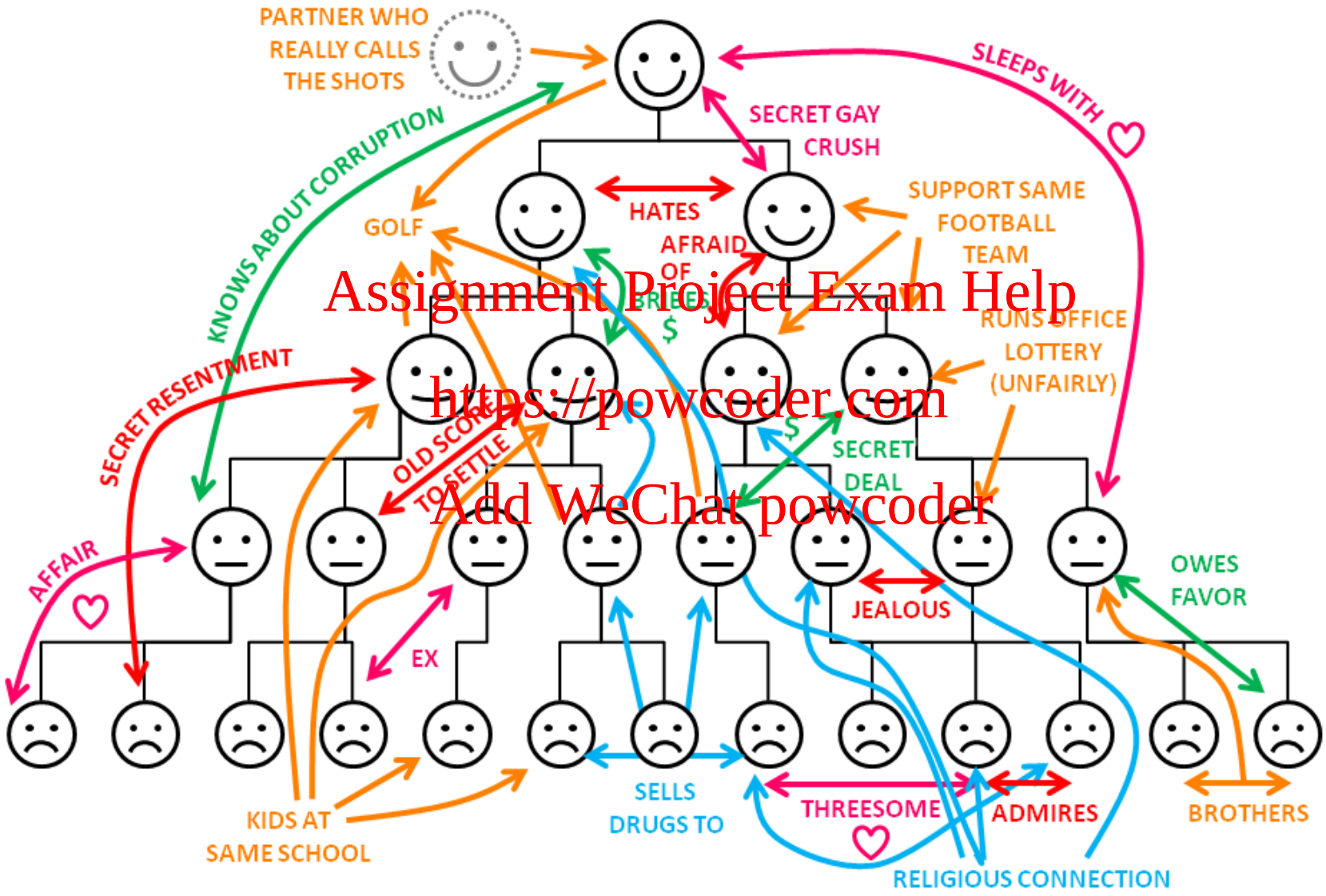
- Technical Users Account for 86% of all attacks
- 90% had systems administrator or privileged system access
- most crimes were committed by insiders **following termination**. Most incursions -- 64% -- involved VPNs **and old passwords that had never been terminated**
- The impact of the attacks is 10x greater than from external sources
- 30% have a prior history

Organization Chart

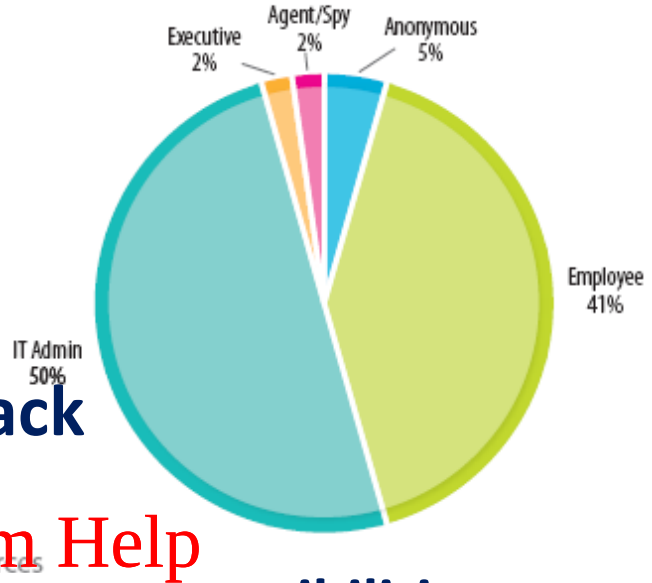


REAL ORGANISATION CHART

INTEGRATION TRAINING
www.integrationtraining.co.uk



Attack Metrics



- Unauthorised access at time of attack
  - Accounts not disabled
  - User rights not changed when employee responsibilities changed
- 31% of cases attackers used their own credentials
- 33% of attacks used another employee's credentials
- 56% of cases another account was compromised
- 17% of attackers used back-door accounts
- 15% used sys admin accounts

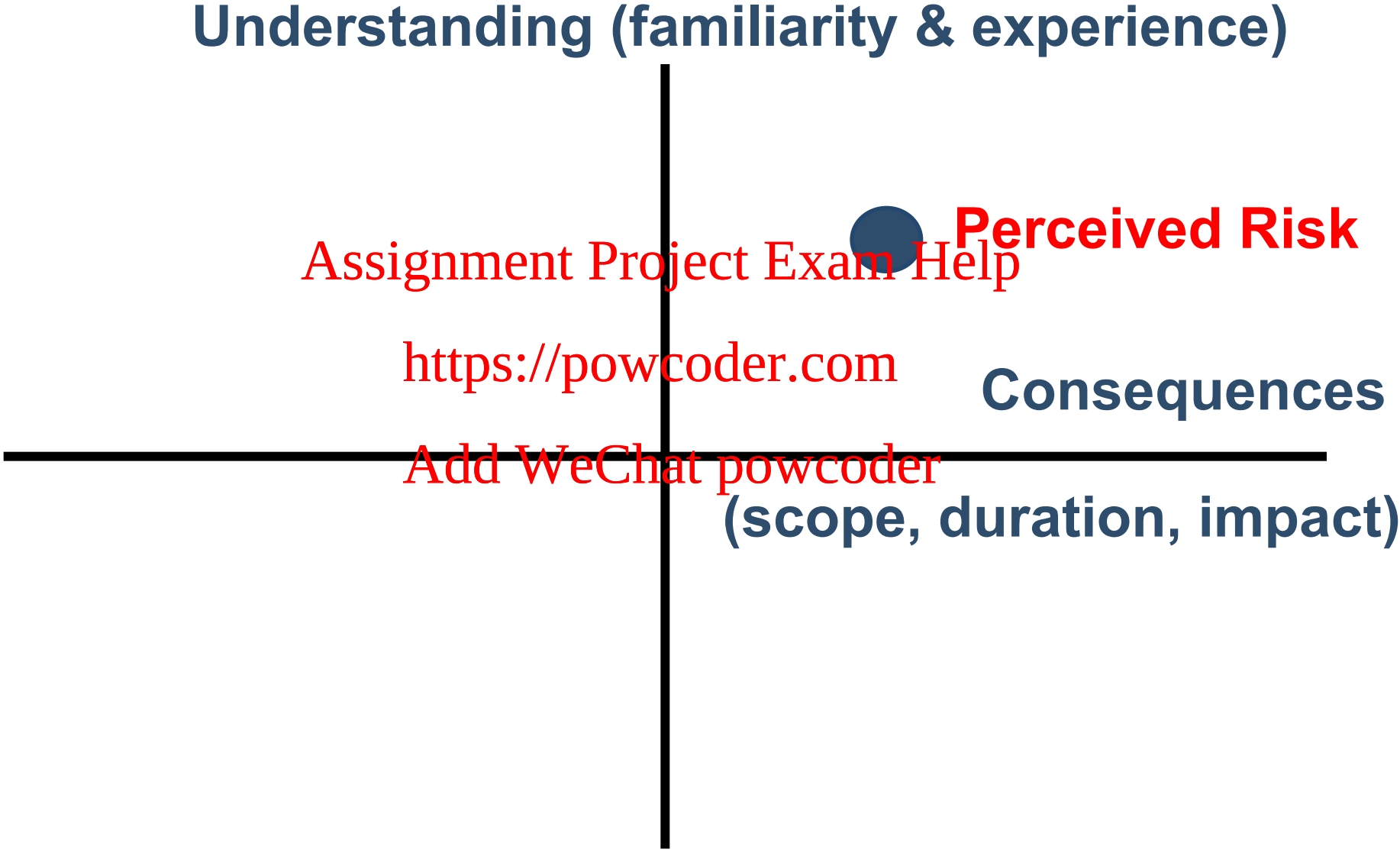
Methods Used

- Logic Bomb
- Back door accounts
- Virus/Malware
- Remote sysadmin tools
- Using other people's credentials
- Elevated Privileges

Dark Triad

Insider Misbehaviour Motivations

- Espionage
- Sabotage
- Theft of Intellectual Property
- Financial gain
- Revenge
- Curiosity/Because they can
- Vanity



Understanding

- Level 1 – judge the value of the materials
- Level 2 – can they detect a pattern
- Level 3 – can they distinguish between facts and inferences
- Level 4 – can they use the info in a new situation
- Level 5 – can they recall data or information

Consequences

- Level 1 – Trivial
- Level 2 – Recoverable
- Level 3 – Serious and long term
- Level 4 – Raise deep concerns
- Level 5 - Catastrophic

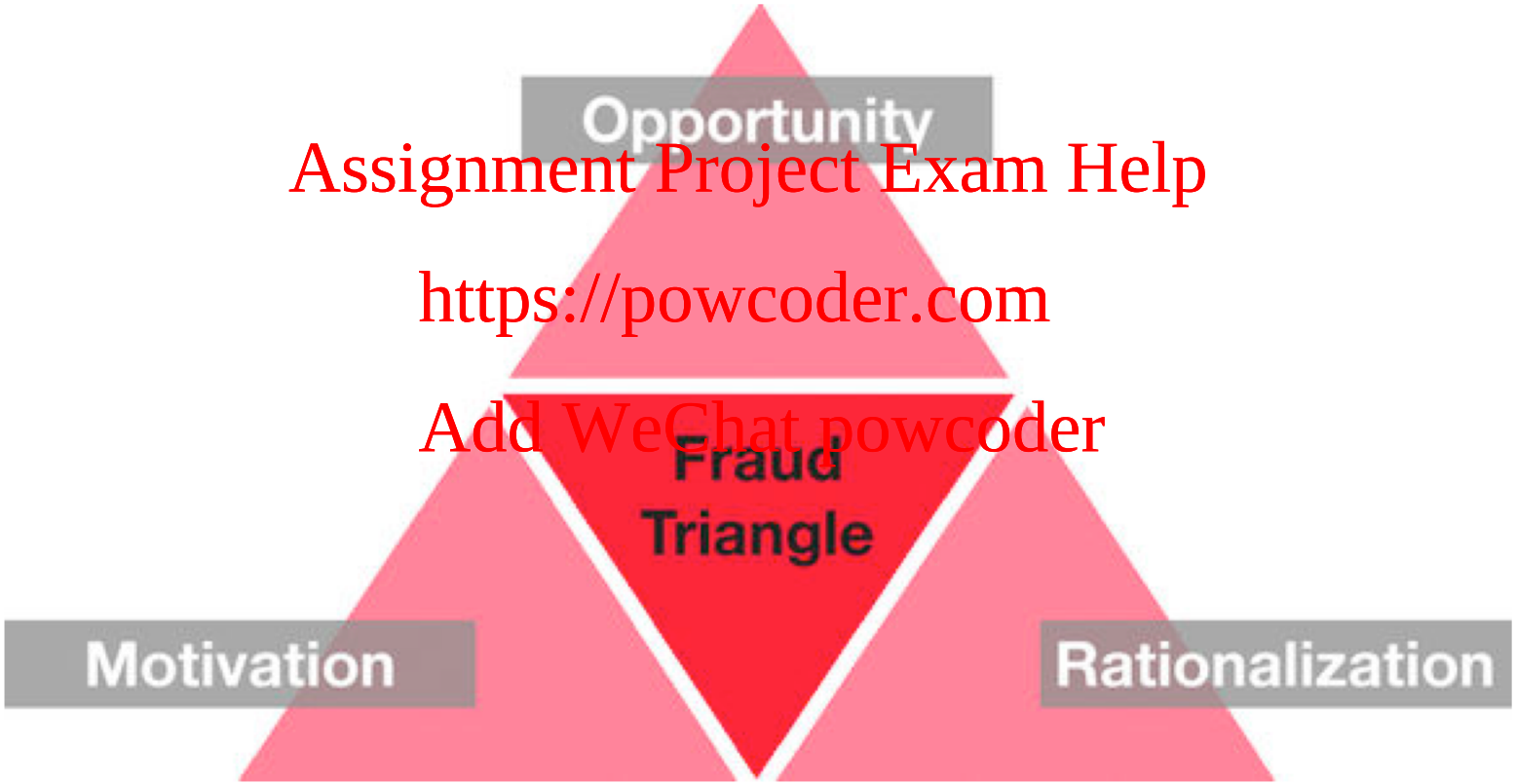
Insiders use Effect Heuristic

- Shortcut – allows people to make decisions quickly
- Emotion influences decisions
- Eg lung cancer -> dread
- Instinct based reaction
- Thus the higher the benefit the lower people see the risk as
- No focus on realistic statistics – I won't get caught!

Two biases

- **Isolation Errors**
  - **Prediction of future outcomes biased by scenarios of success**
  - **Past results ignored**
- **Perceived benefits seem to outweigh perceived risks**

Fraud Triangle



Motivation

- **Pressure/non-Shareable financial problems**
  - **Unable to meet obligations**
  - **Personal failure**
  - **Business reversals**
  - **Physical isolation**
  - **Status gaining**
  - **Employer-employee relations**
- **Mostly status seeking or status maintaining**

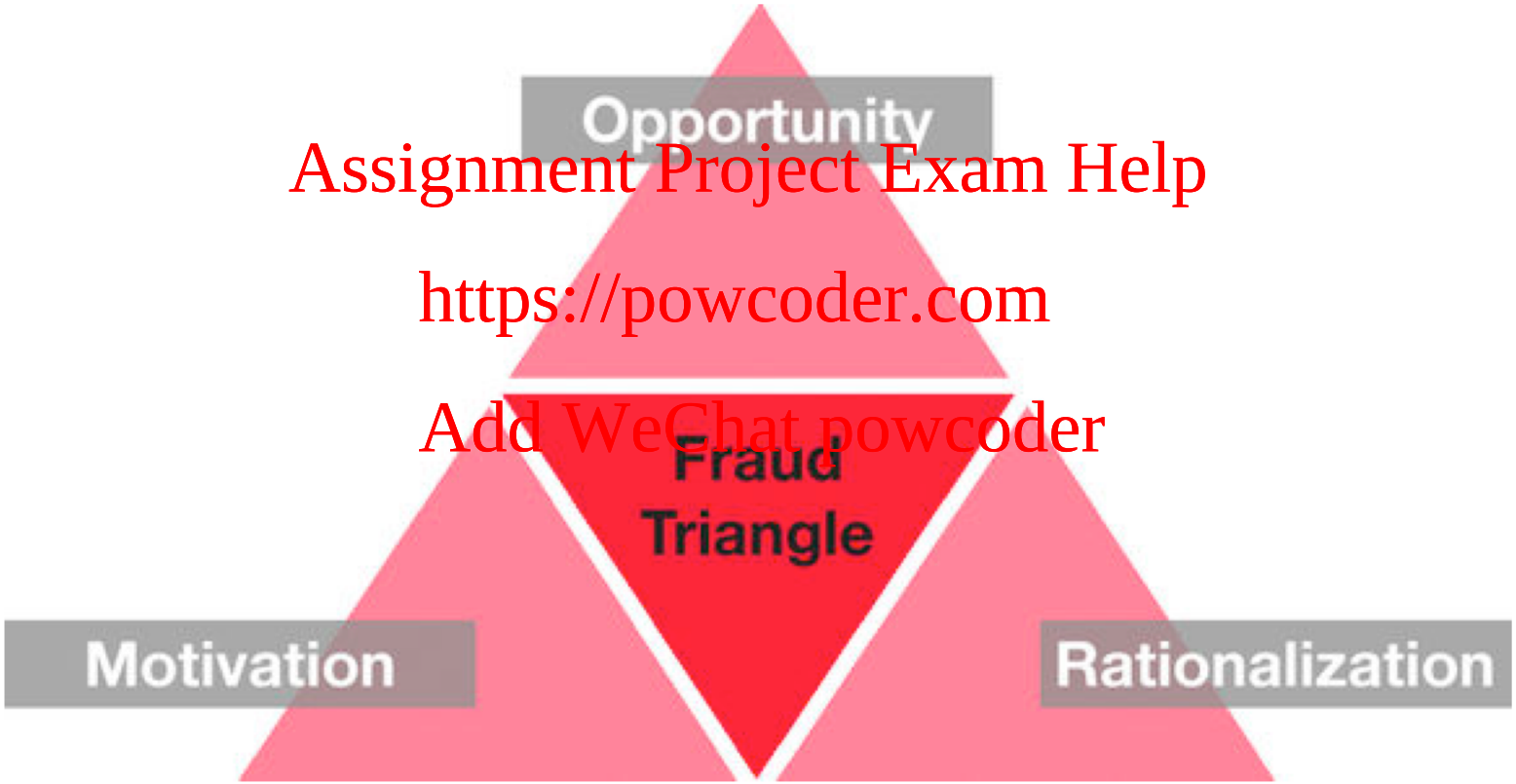
Opportunity

- Technical Skills
- Position of trust
- Hearing about other violations
- Getting access to someone else's password

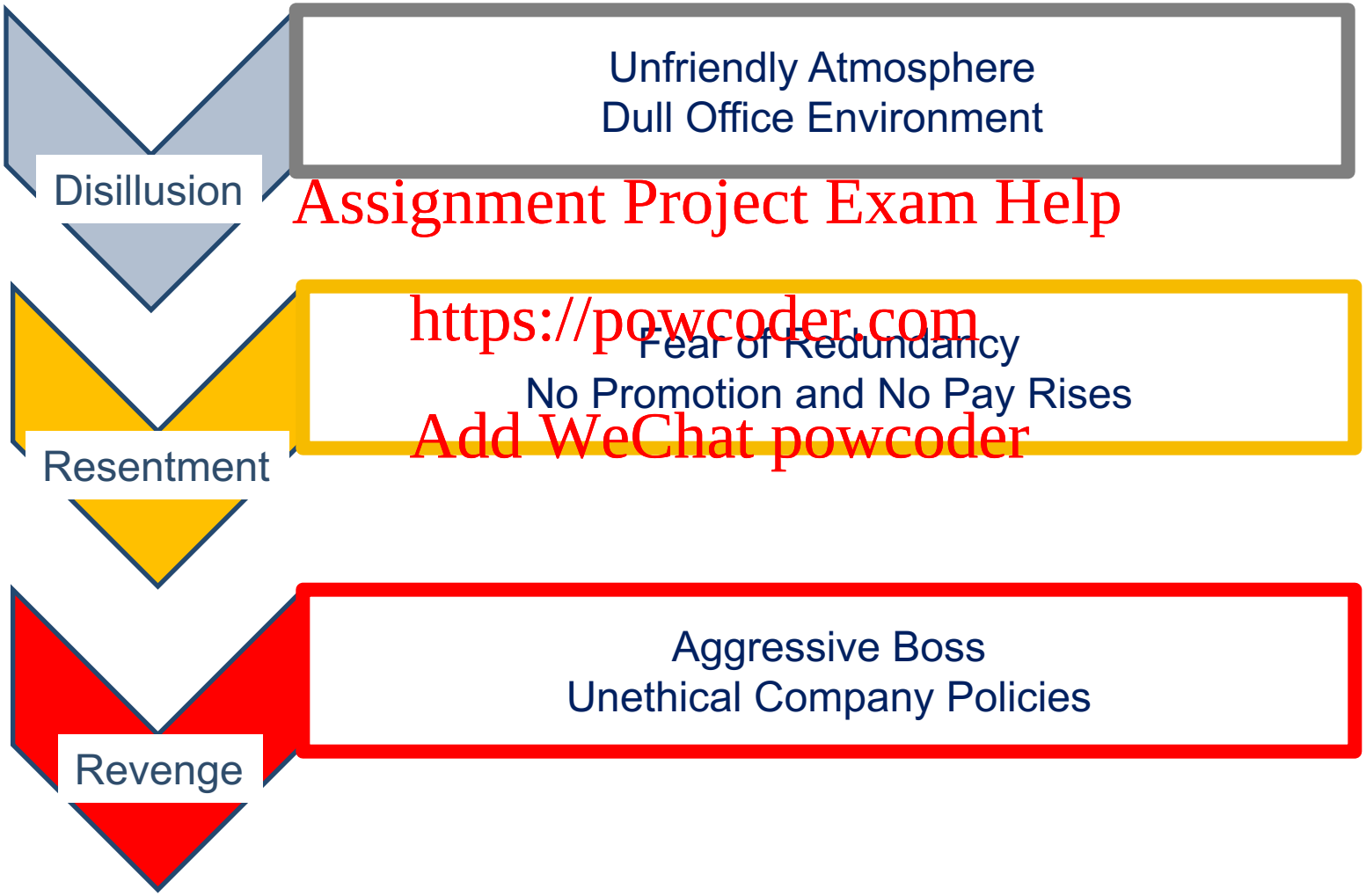
Rationalisation

- Insiders view themselves as
  - Non criminal
  - Justified
  - Part of general responsibility in the organisation

Fraud Triangle



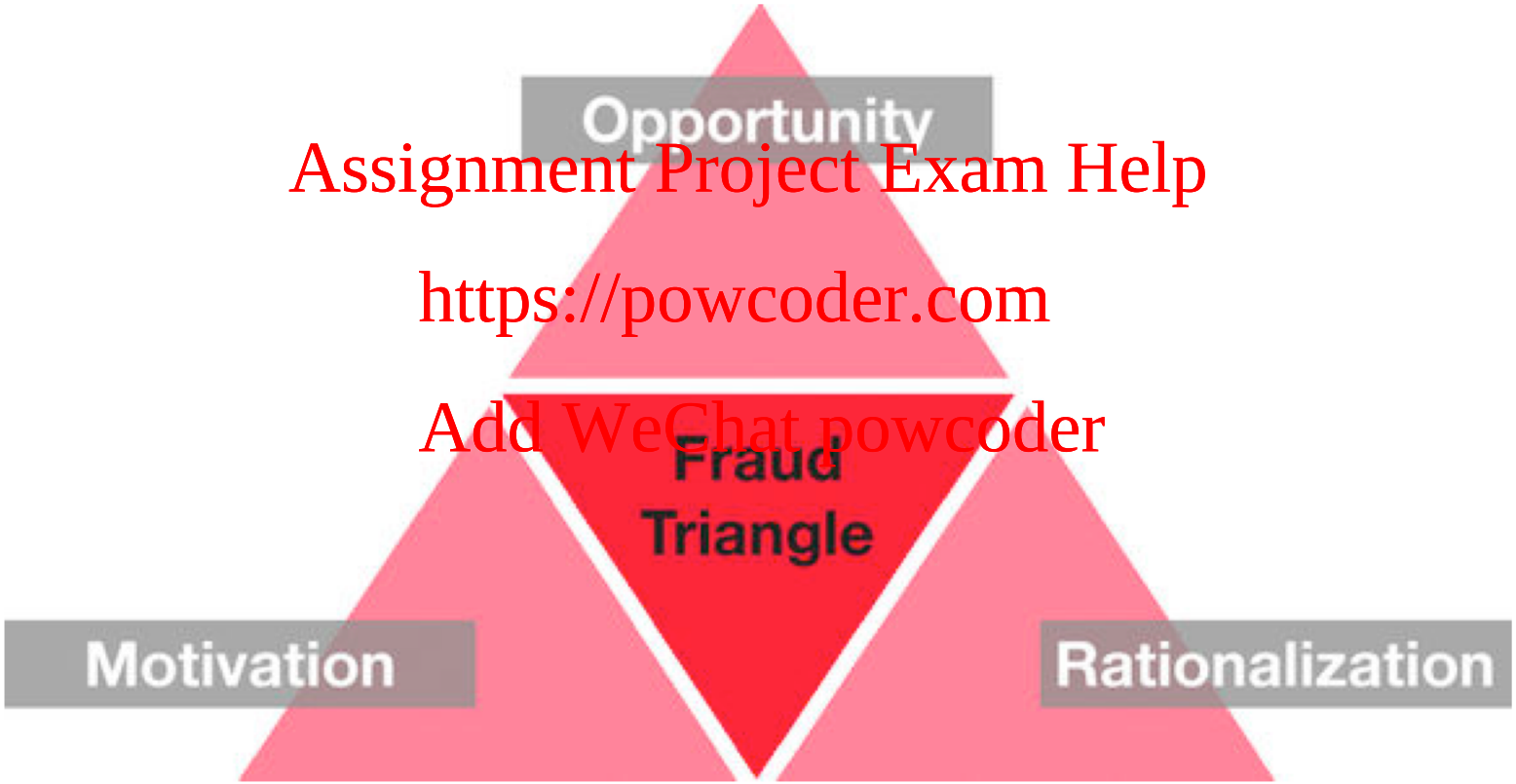
Path to Revenge




Assignment Project Exam Help
https://powcoder.com
Add WeChat powcoder

Insider Threats

Fraud Triangle



Motivation

- **Pressure/non-Shareable financial problems**
  - **Unable to meet obligations**
  - **Personal failure**
  - **Business reversals**
  - **Physical isolation**
  - **Status gaining**
  - **Employer-employee relations**
- **Mostly status seeking or status maintaining**

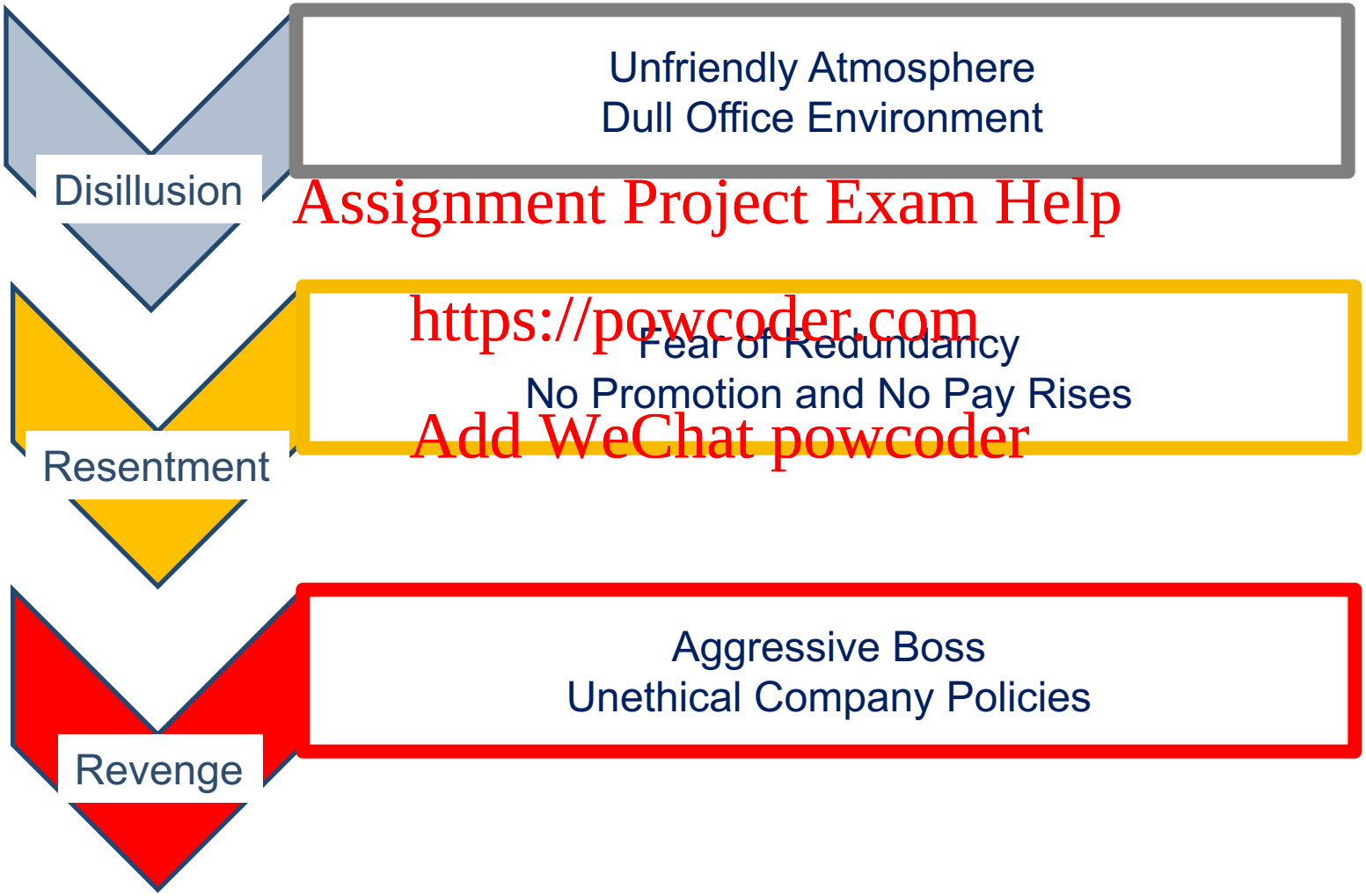
Opportunity

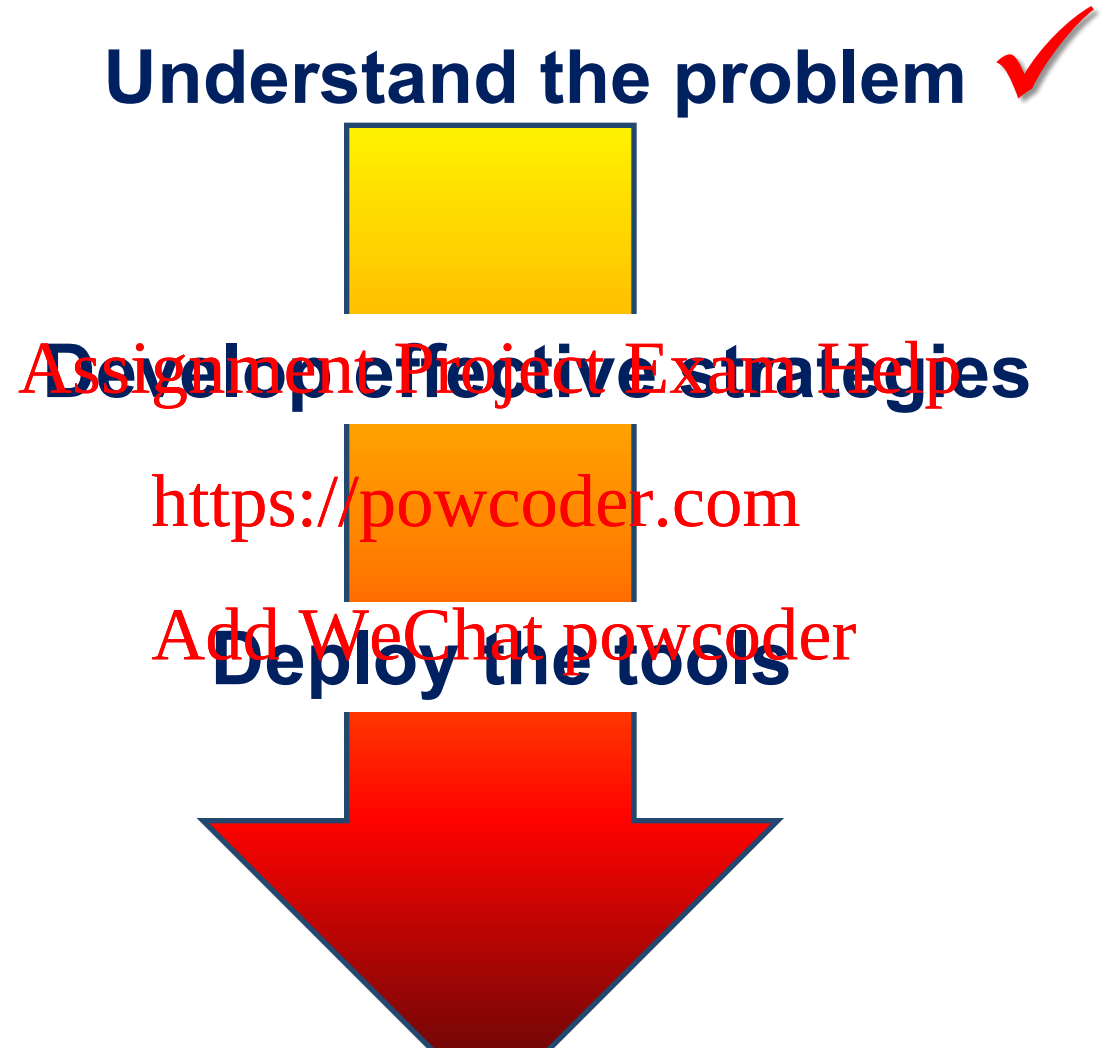
- Technical Skills
- Position of trust
- Hearing about other violations
- Getting access to someone else's password
- Poor Management Practices

Rationalisation

- Insiders view themselves as
  - Non criminal
  - Justified
  - Part of general responsibility in the organisation

Path to Revenge





Mitigation

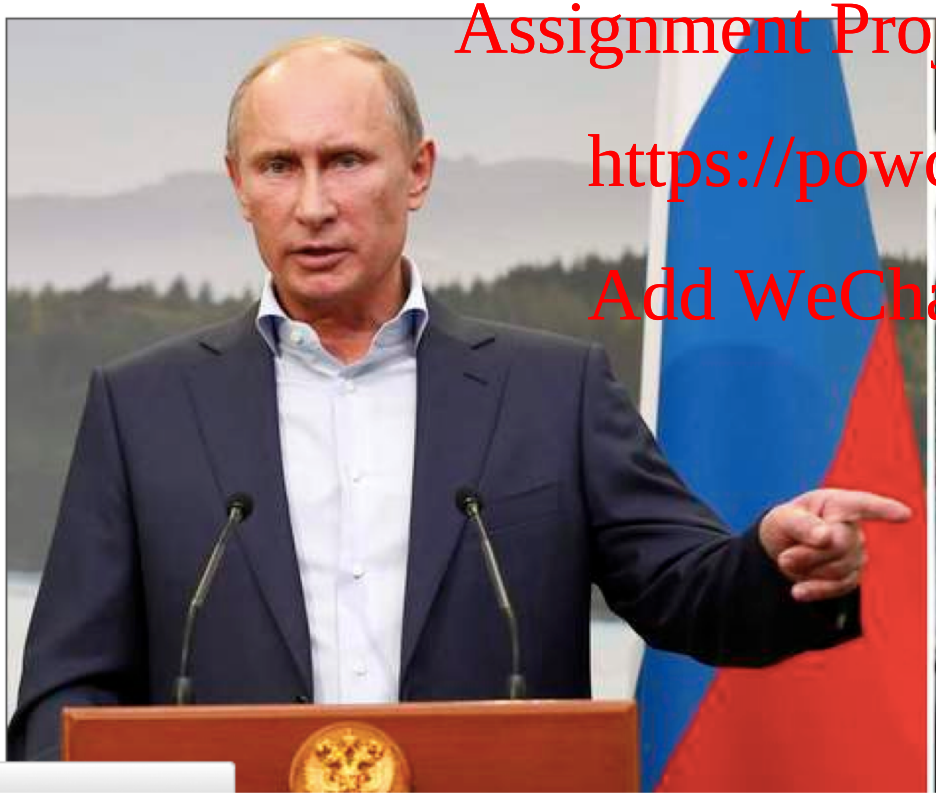
1. Understand Risk of Detection (and do it)
   - Employee Education
   - Proactive Detection
2. Create a fair working environment

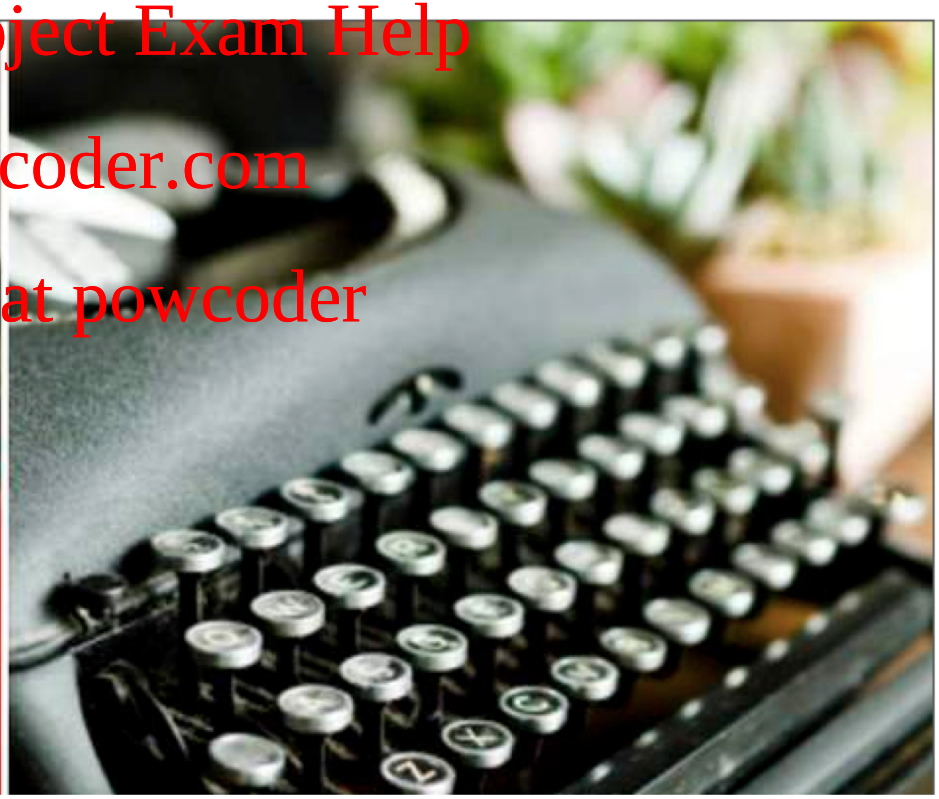
Russia's Approach

Kremlin Typewriters: Russian Plan To Stop Leaks

A Kremlin agency looks to safeguard Russia's security by ditching computer hardware for old-school typewriters.

11:36am UK, Saturday 13 July 2013

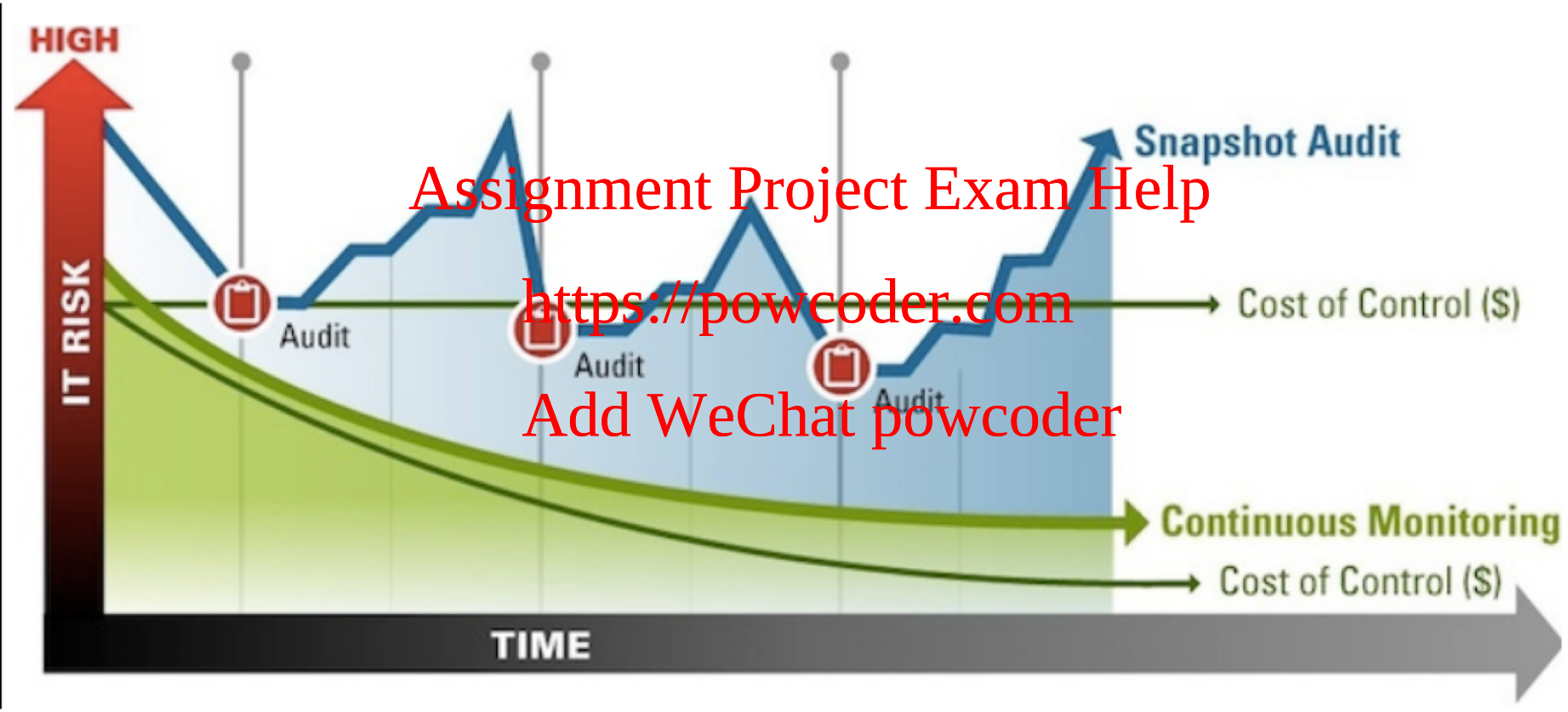




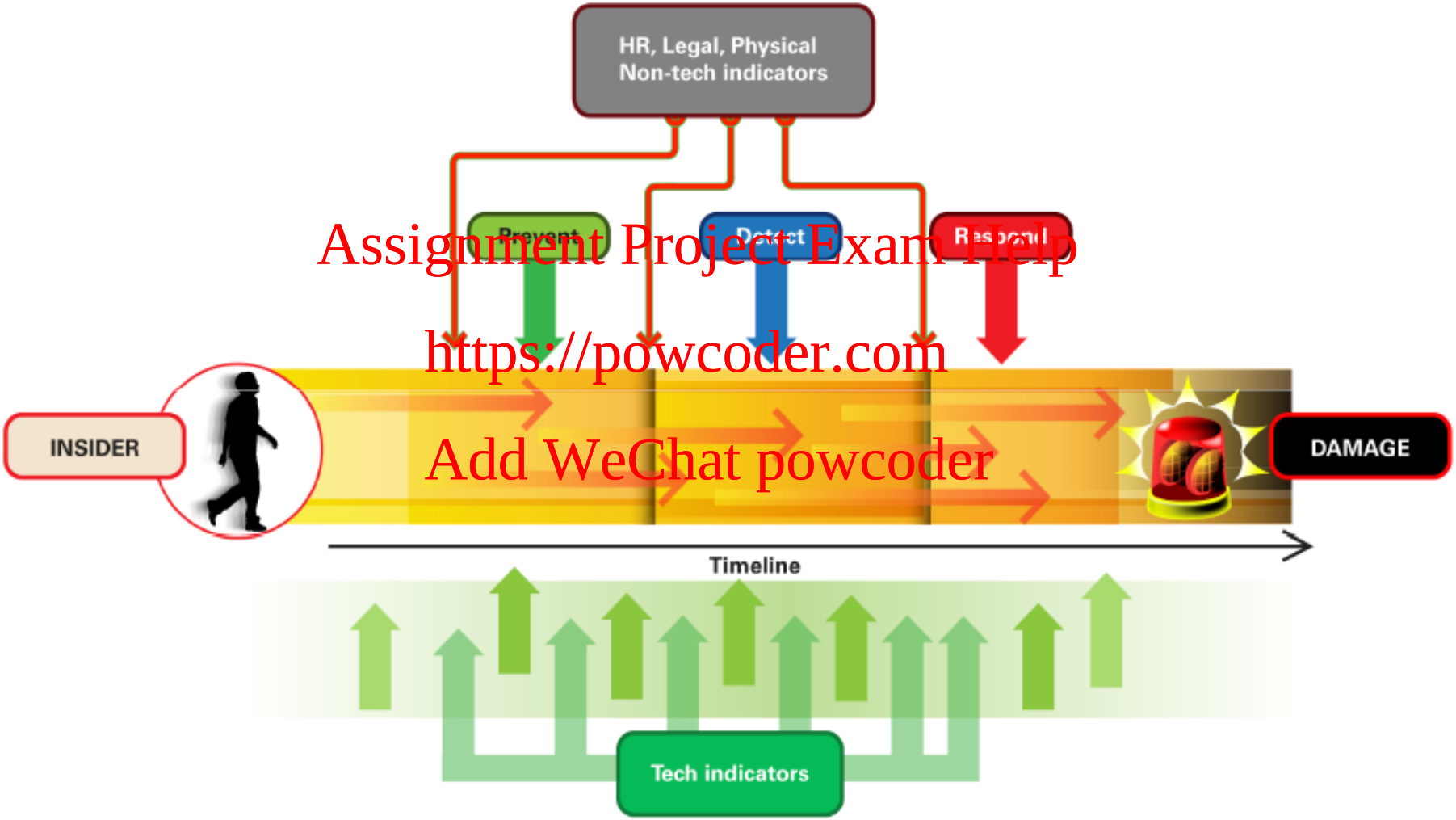
All is not visible…

- Use software tools
- And soft tools

Continuous monitoring



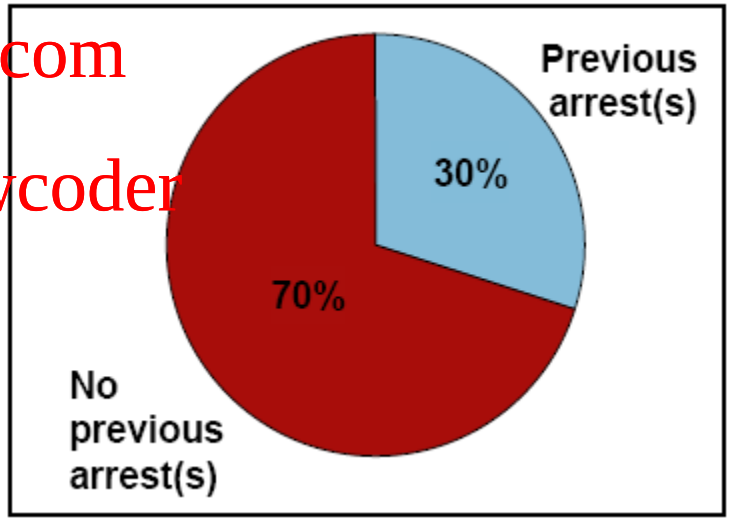
CERT Insider Threat Center Objective



Opportunities for prevention, detection, and response for an insider attack

Employee Profiling (Prevention)

- Employee profiling could be carried out pre-hire
  - Fast and Legal
  - Also do a background check on new employees
  - Check CVs
- Prevents
  - Wrongful termination
  - Financial Loss
  - Embezzlement
  - Workplace disruption
  - Injury claims
- Check external contractors too



Need a Policy for Insider Threat Mitigation

- **Prevent:**
  - **Pre-hire practices**
- **Detect:**
  - **Red Flag Events**
    - **What should bosses look out for?**
    - **What should they do when these events occur?**
    - **Access control practices**
- **Respond:**
  - **What Interventions?**
  - **Termination practices – what needs to be done?**
- **Tools needed**
    - **Outsourcing?**

Detection & Response

Insider Threat Management

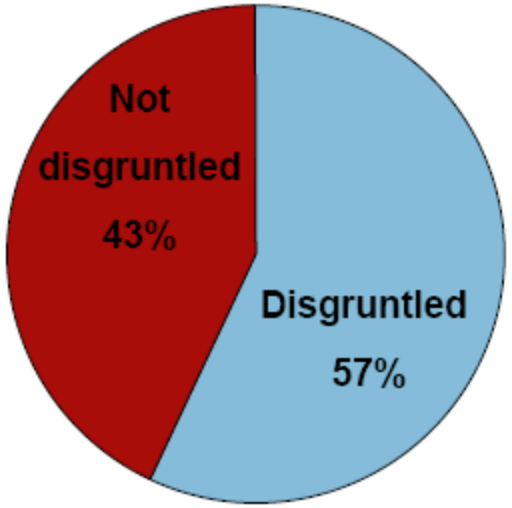
- **Prevent:**
  - **Principle of least privilege**
  - **Separation of duties**
- **Detect**
  - **Log, monitor and audit employee activity**
  - **Special attention to admins and privileged users**
  - **Allow anonymous reporting of issues**
- **Respond**
  - **Termination procedures essential – lots of incidents from non-employees**
  - **Retain all logs to support investigations**

What the Research tells us:

- Insiders are often disgruntled (57%)
  - Disgruntlement level
- Insiders often attacked following a negative event (92%) – dispute, demotion, transfer
  - Precipitating event
- Insiders exhibit concerning behaviour BEFORE the attack (offline)
  - Behavioural precursor
- Many held IT positions (86%)
  - Technical Precursor

Precipitating event

- Overwork or a consistently heavy workload
- Feeling unappreciated or underappreciated
- Conditions of the workplace
- Demanding, rigid supervision that is too involved in the work being done
- Unsupportive, weak supervision that does not offer enough input or guidance
- Unmet expectations
  - Insufficient compensation
  - Lack of career advancement
  - Inflexible policies
  - Supervisor demands/co-worker relations



Behavioural Precursor

- Absenteeism
- Raising the voice frequently
- Depression
- Impatience
- Irritability
- Memory/ Concentration problems
- Paranoia
- Showing up late
- Argumentativeness
- Poor Performance
- Violations of policies/procedures

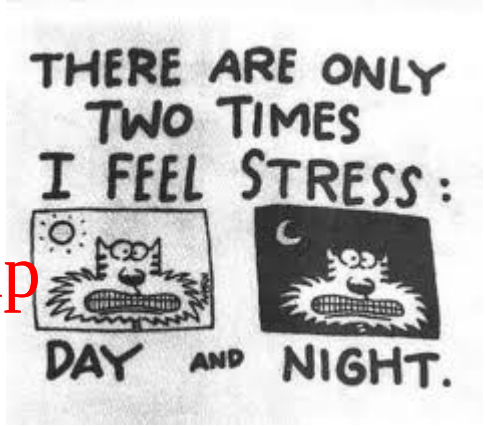
Disgruntlement Predisposition

More info

- People have **expectations** of "freedoms"
- People accumulate **access paths** over time. The organisation easily loses track of these
  - Few formal access path tracking procedures
  - Some are granted, some are fraudulently created
  - People sometimes share access with others to achieve organisational operations
- Majority attacked AFTER termination (59%)

Interventions

- Awareness
- Responding to incidents
  - Offer remediation opportunities
  - Counselling
  - Empower colleagues to provide support
  - Destressing activities
- Continue to Monitor



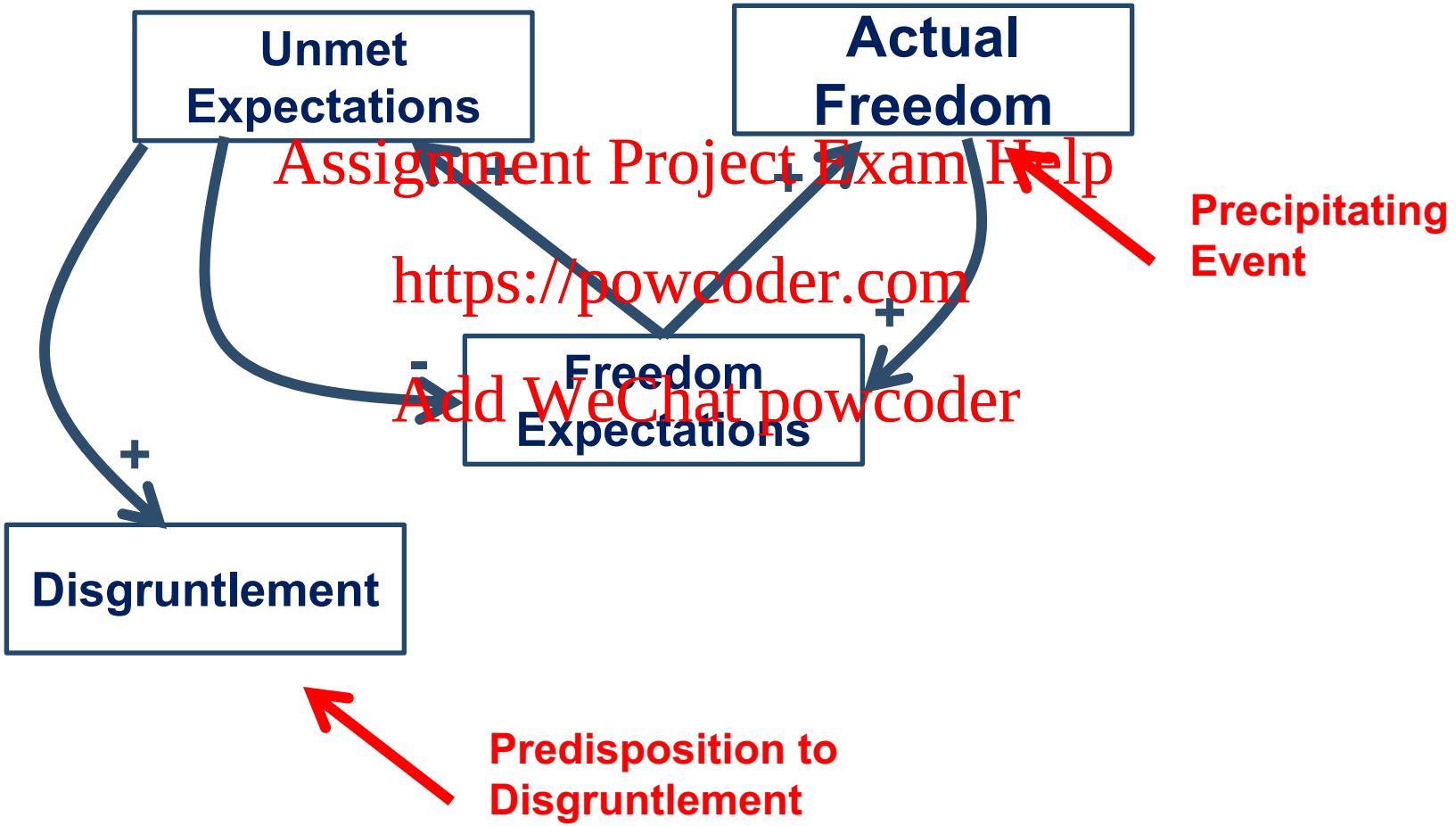
Systems Diagrams

- First identify the stocks
- Then identify the connections between them
- And the causatives
- There are many correct answers!

Draw a Systems Diagram

- **Show interplay between**
  - **Disgruntlement**
  - **Precipitating event**
  - **Freedom Expectations**
  - **Actual Freedoms**
  - **Unmet expectations i.e. discrepancies**
  - **Predisposition to disgruntlement**

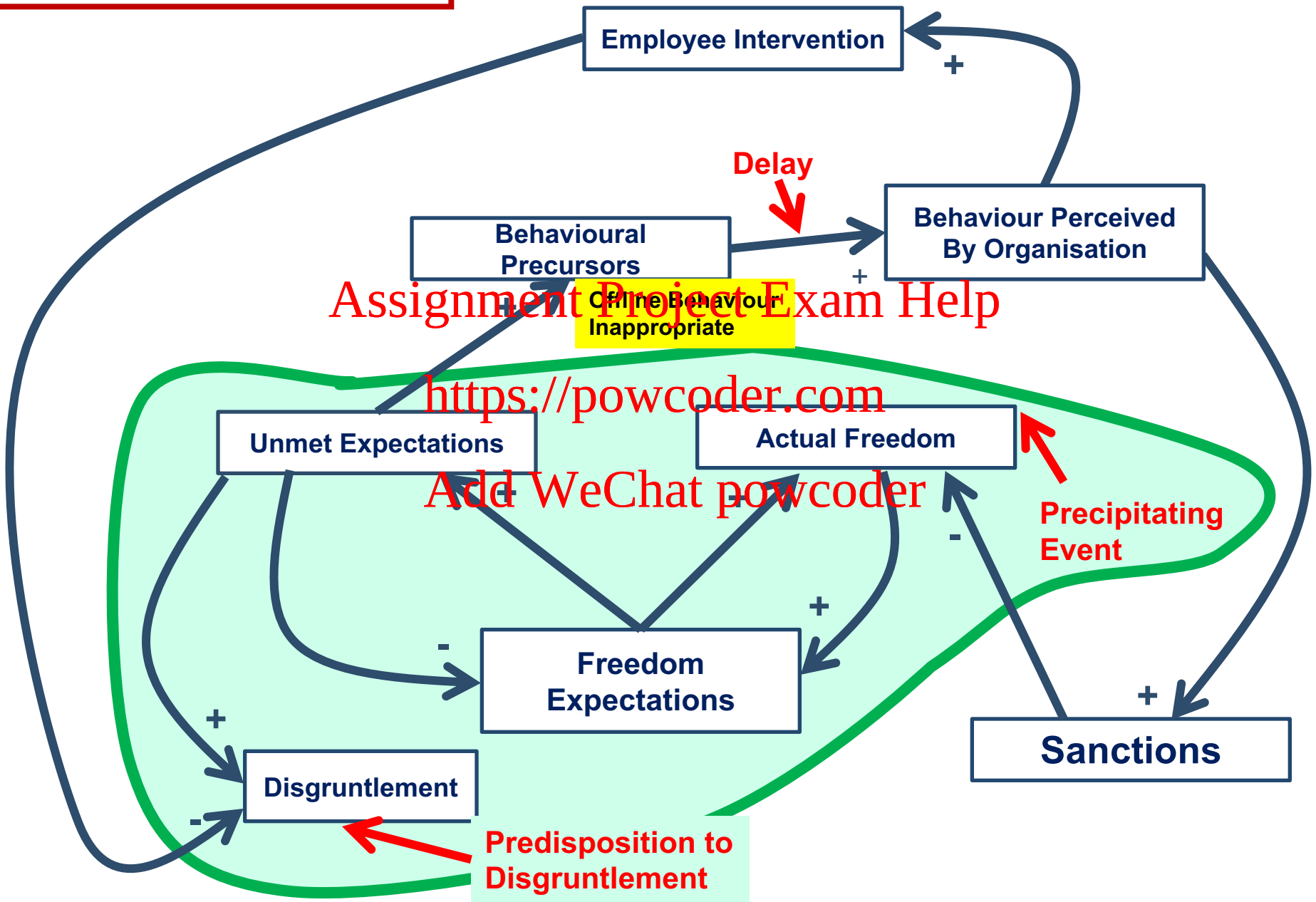
My Diagram



Now add to your diagram

- Behavioural precursors (Inappropriate Behaviour)
- Sanctions
- Employee intervention
- **Delay** (Time to realise insider is becoming a problem)
- Behaviour Perceived by organisation

My Diagram

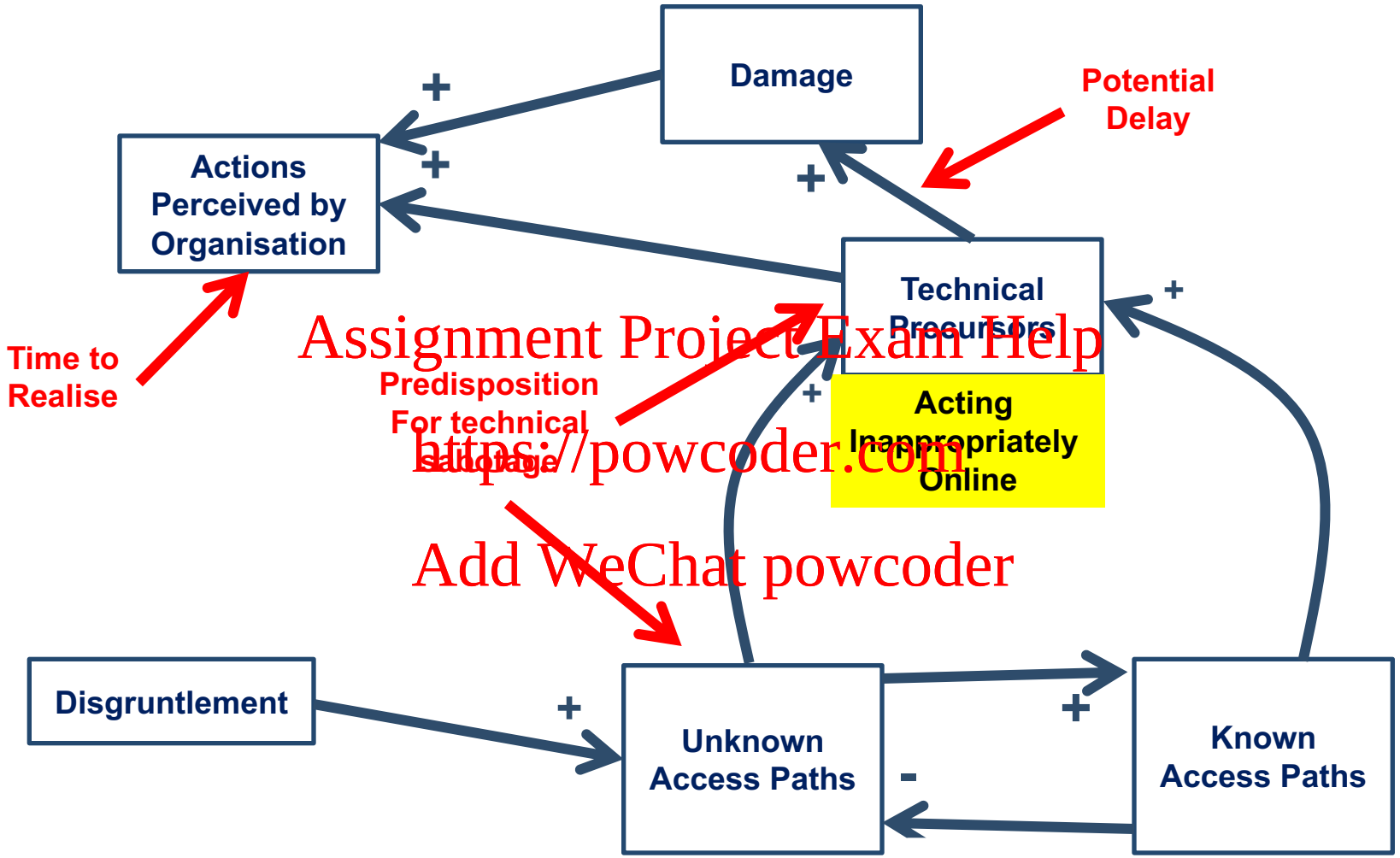


- **Attackers have a sense of entitlement. This escalates over time.**
  - **If curbed, this could lead to resentment**
  - **If not curbed, entitlement increases**
- **Interventions:**
  - **Counselling**
  - **Sanctions**
  - **Technical Monitoring**
- **Termination**
  - **Time period for behaviour to become serious enough**
  - **Time to close all access paths**

New Diagram

- **Show interplay of**
  - **Known access paths**
  - **Unknown access paths**
  - **Damage**
  - **Disgruntlement**
  - **Technical misbehaviours**
  - **Actions perceived by organisation**
  - **Delay (for organisation to realise)**
  - **Predisposition for technical sabotage**

My Diagram



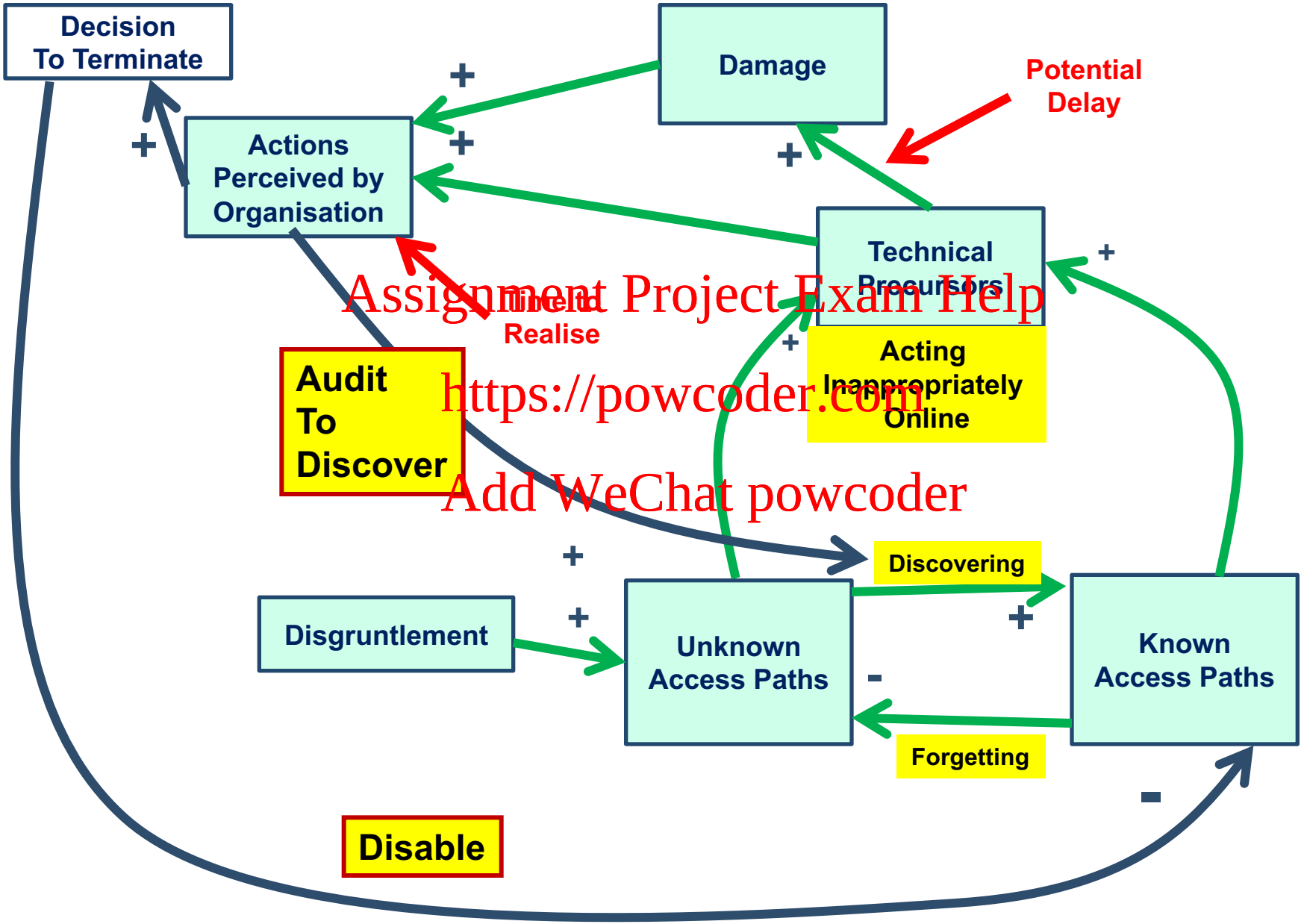
Attack Starts....

- Insider starts acting inappropriately online
  - Accessing unauthorised material
  - Getting more privileges
  - Stealing material
- It takes time for the organisation to realise this is happening
- Organisation hampered in dealing with this
  - By not knowing paths
  - When they do find out, they act to remove them
  - They might not know about logic bombs

Add to your Diagram

- **Audit**
- **Termination**
- **Actions upon termination i.e. disabling access paths**

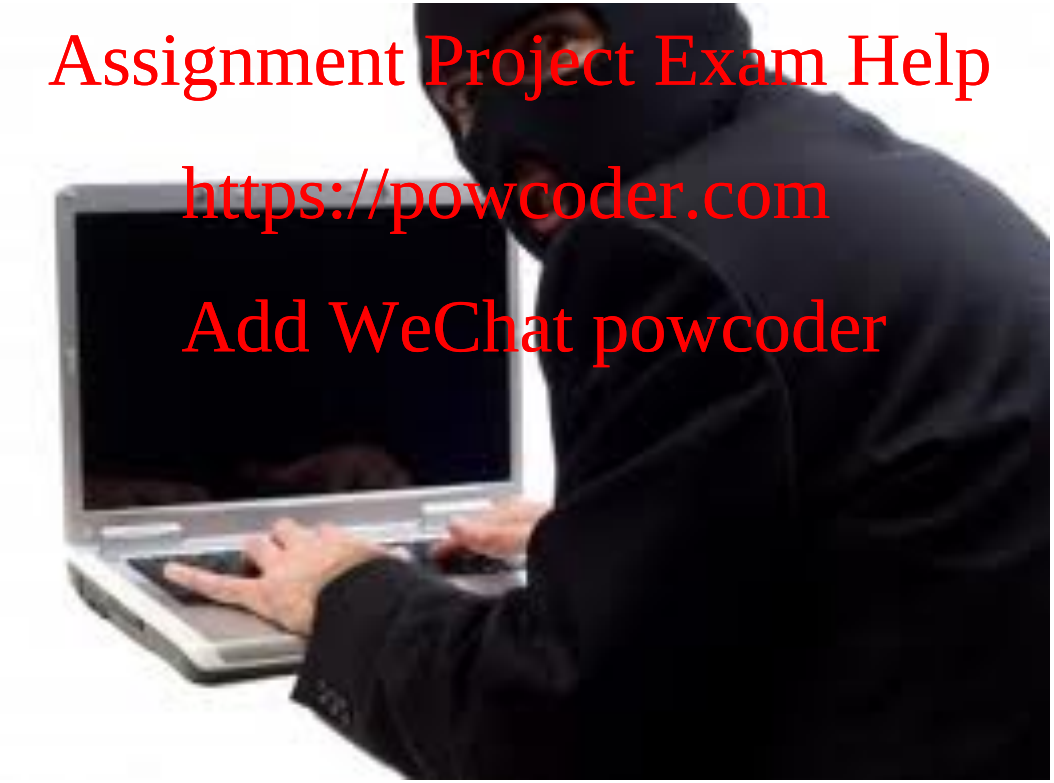
My Diagram



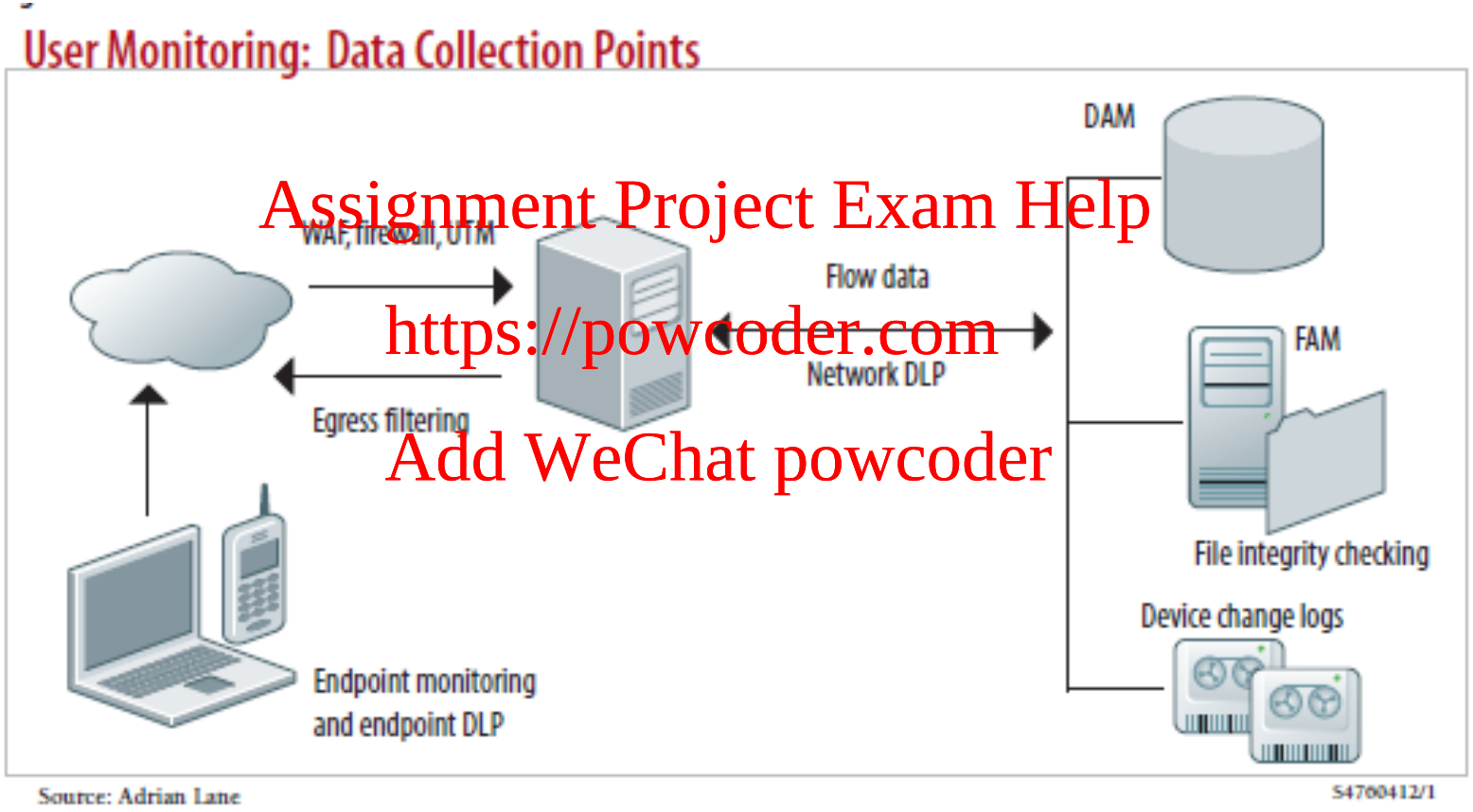
Task

- **Pre-employment Checks (red)**
  - **Low risk, medium risk and high risk.**
- **Non-technical (blue)**
  - **Non-technical actions that companies take to guard against insider threats.**
- **Technical (green)**
  - **Technical actions that companies take to guard against insider threats.**

Technical Tools/Monitoring



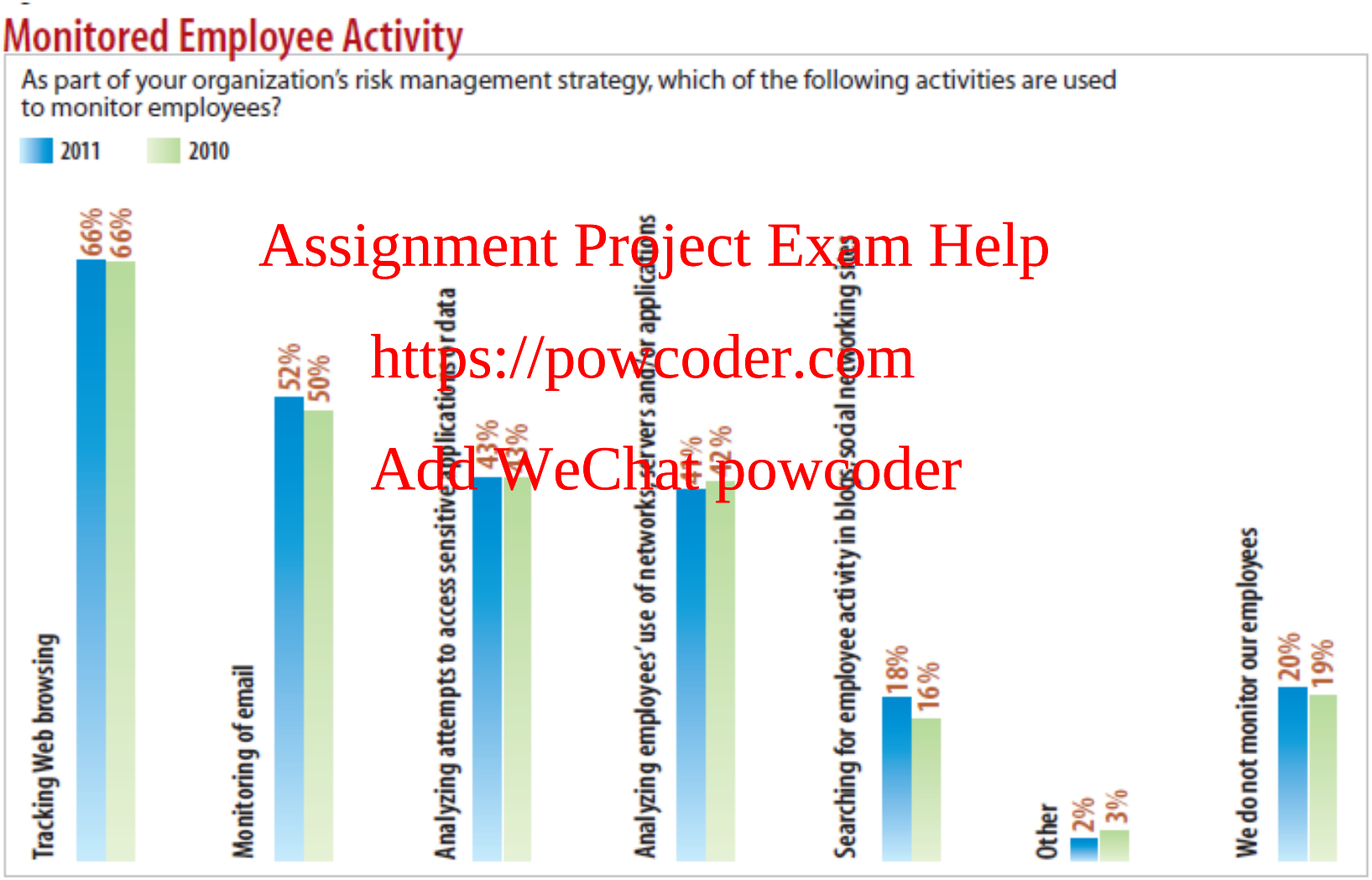
Employee Monitoring

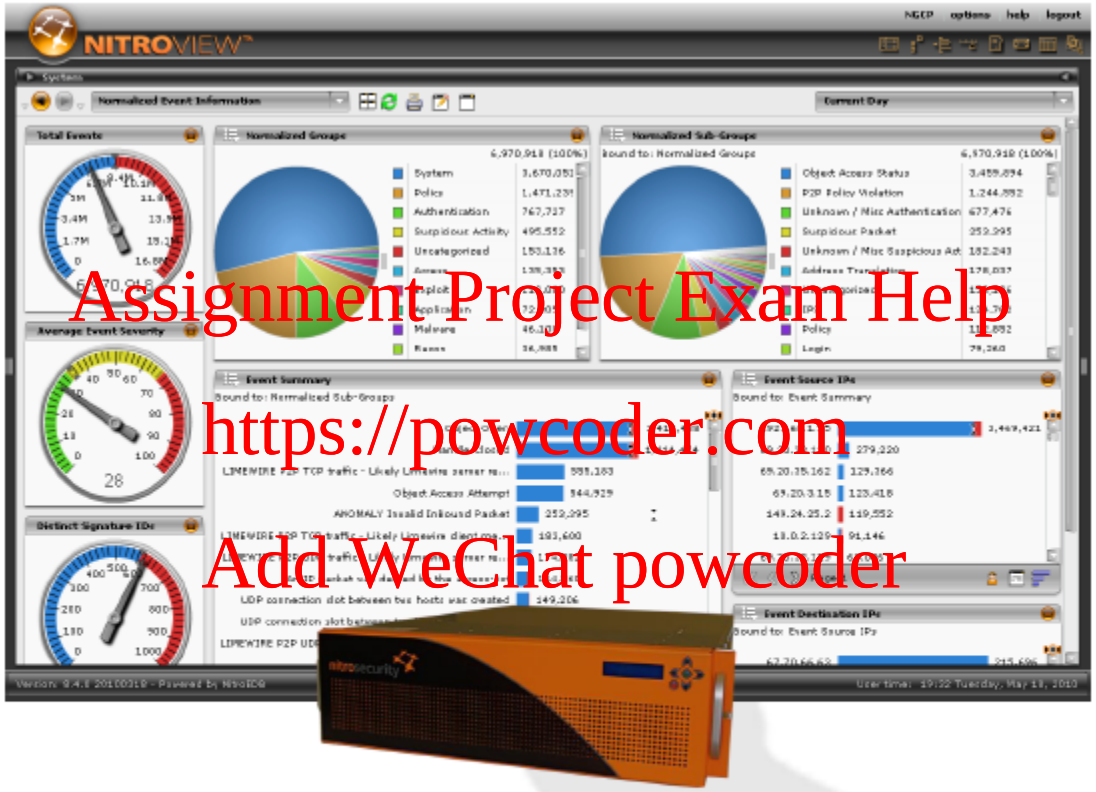


Employee Monitoring

- Specific Actions
  - Files accessed
  - Databases used
  - Network access
  - Check against policies and alert if violation
- Monitor behaviour and compare to historic usage patterns
  - Is it different from usual?
  - Eg – download the whole customer database instead of only one customer

InfoWeek Strategic Security Survey





Insider Threat Detection Technology

Content-Aware Forensics & Breach Discovery

A user performs a query against a SQL server resulting in a recordset exceeding a threshold of 1000 rows or from a privileged table. This represents a data access policy violation.

The offending user prints the resulting SQL query results to a PDF document which is then attached to an email using a Google web account and sent to an unauthorized external address without the corporate email disclaimer.

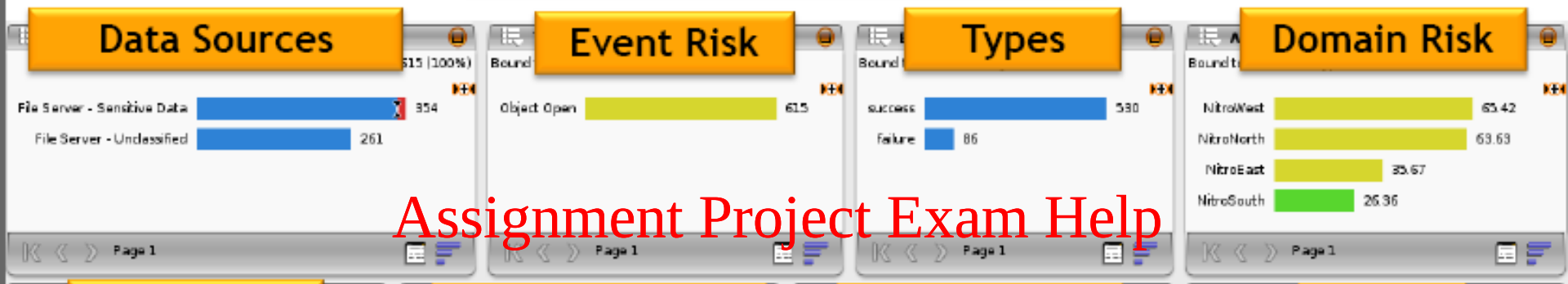
The suspect user proceeds to have an IM chat to a IM userID NOT registered on the whitelist of authorized IM user names to discuss the sensitive data obtained and sent via email.

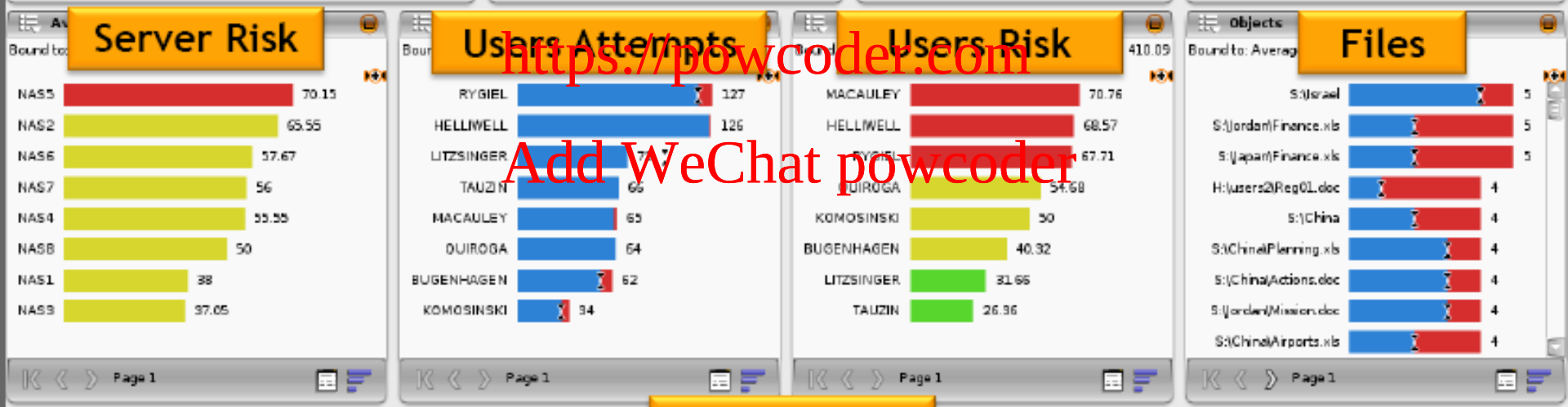
Forensic evidence obtained from this activity

1. SQL session history including details from all transactions performed during the suspicious user activity
2. MIME-decoded email record complete with From/To Address, Subject, Message and document Attachment
3. IM session data and a transcript of the IM conversation dialog
4. Identity of offending internal, topology-specific switch/port location, current (and all prior) IP address usage and current network session state.

File Monitoring Analysis Console

Operational Console
Total Environmental Awareness





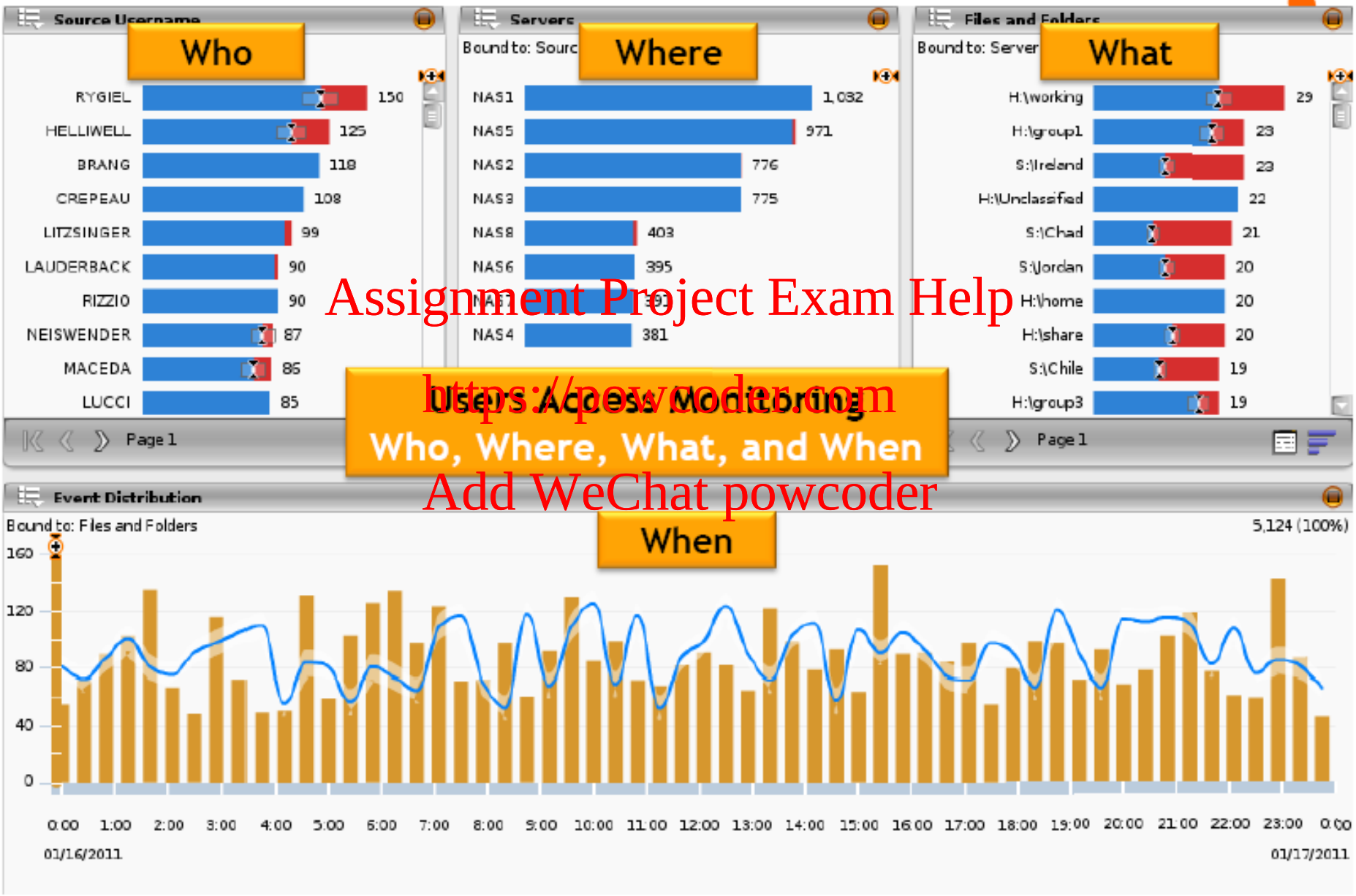
The Details

Events

Bound to: Objects

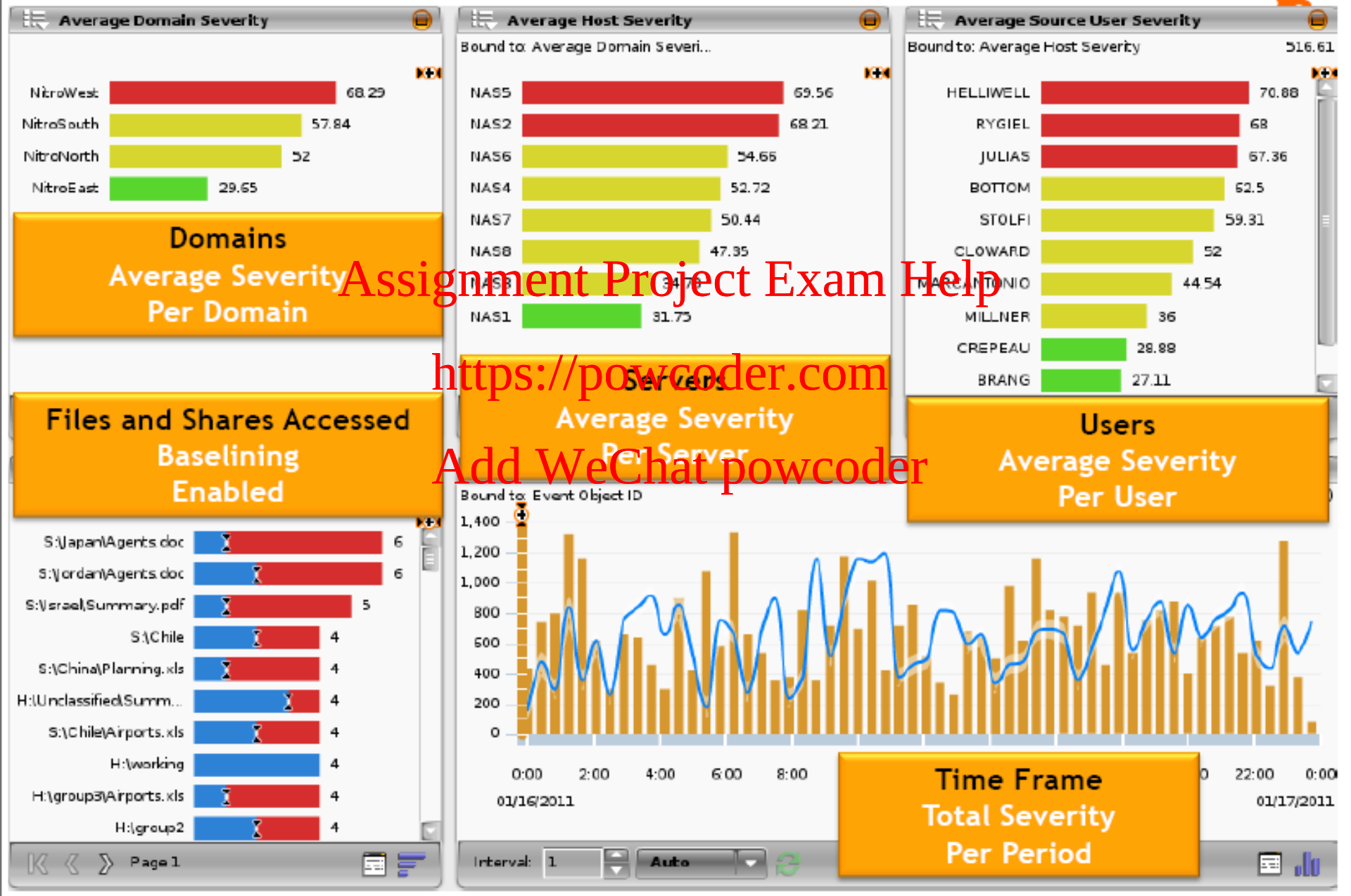
Severity	Source User	Object	Rule Message	Event Subtype	Source IP	Last Time	Domain	Host
20	BUGENHAGEN	H:\pages\BOD.doc	Object Open	failure	69.20.154.152	01/06/2011 13:06:49	NitroEast	NAS5
20	LITZSINGER	H:\users3\BOD.doc	Object Open	success	69.20.154.152	01/06/2011 13:01:49	NitroEast	NAS3
80	MACAULEY	S:\China	Object Open	failure	69.20.154.153	01/06/2011 13:00:32	NitroNorth	NAS2
80	HELLWELL	S:\Guam\Mission.doc	Object Open	success	69.20.154.153	01/06/2011 13:00:32	NitroWest	NAS4
20	LITZSINGER	H:\users2\Reg01.doc	Object Open	success	69.20.154.152	01/06/2011 12:46:49	NitroEast	NAS3

User File Access Distribution

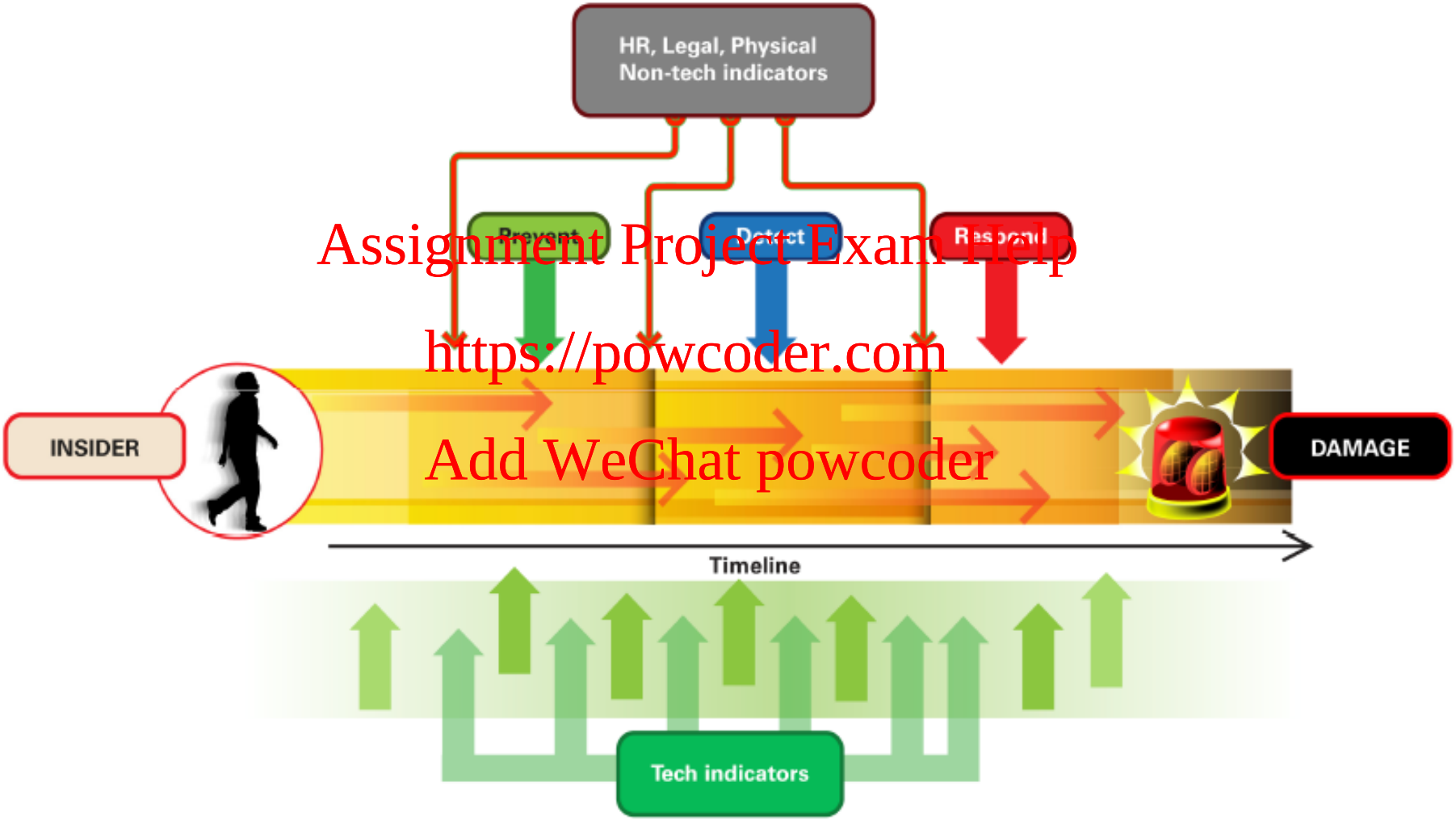


User Access Monitoring
Who, Where, What, and When

Domain Severity Indicators Drill Down

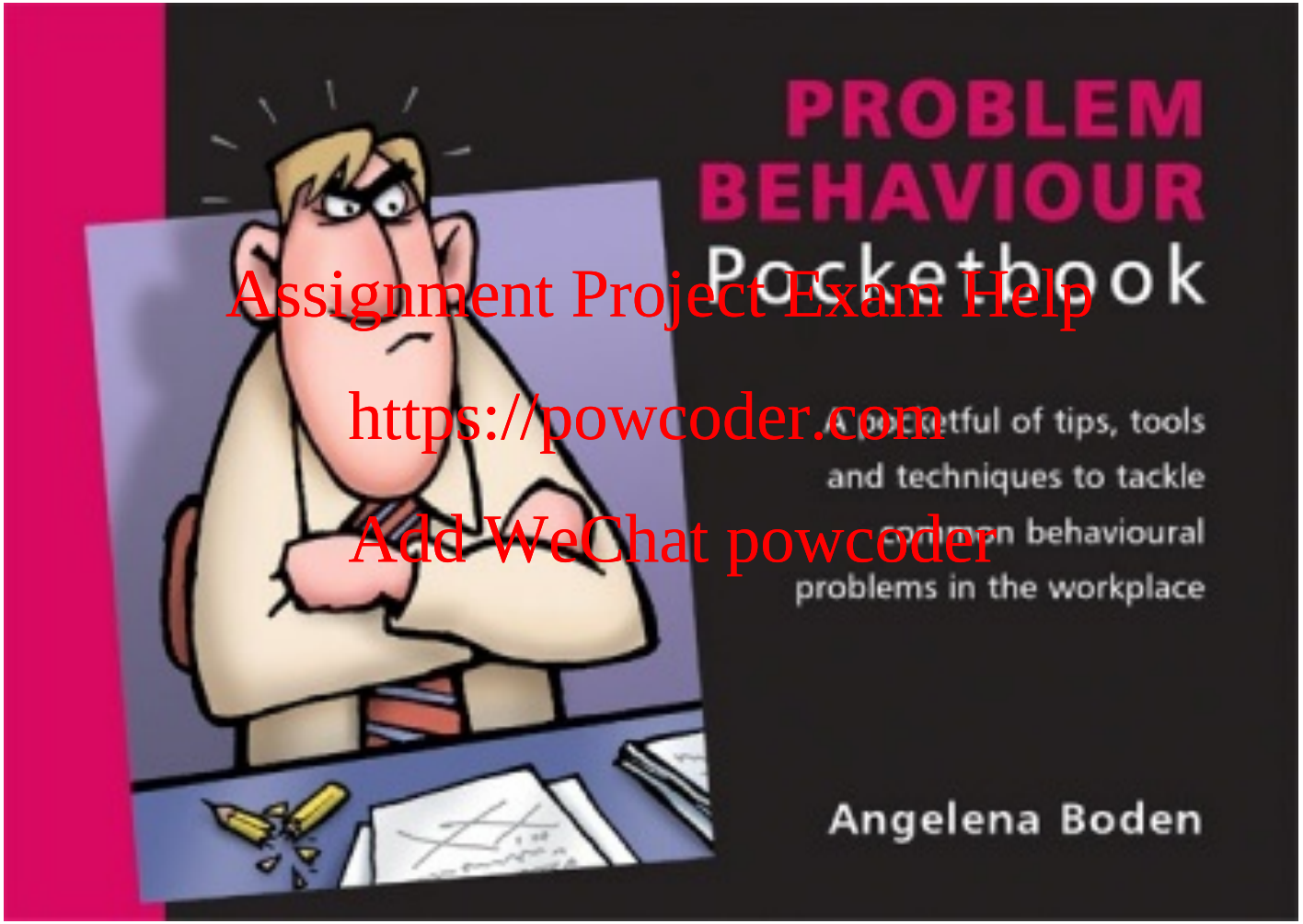


CERT Insider Threat Center Objective



Opportunities for prevention, detection, and response for an insider attack

Soft Tools



CERT Resources

- Insider Threat Center website (http://www.cert.org/insider_threat/)
- Common Sense Guide to Mitigating Insider Threats, 4th Edition (http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm)
- Insider threat workshops
- Insider threat assessments
- New controls from CERT Insider Threat Lab
- Insider threat exercises

MERIT Model of Insider IT Sabotage