TALES FROM THE WAR ROOM VERSION 0.1

TF-CSIRT/FIRST Symposium, Hamburg, Germany

January 26, 2010

Notes from the Session:

- Thanks! To all who attended and participated in our experiment. I think this was worthwhile and hope to have the chance to do it again.
- I've inserted some notes and comments that were captured during our session and included them in this handout slide deck.
- Your feedback on the session, and thoughts on how to continue this dialogue could be continued is welcomed. I'll collect all email addresses you send me, and if we're able to create a mail list, I'll populate it accordingly.

John Snyder CSIRT.core@gmail.com

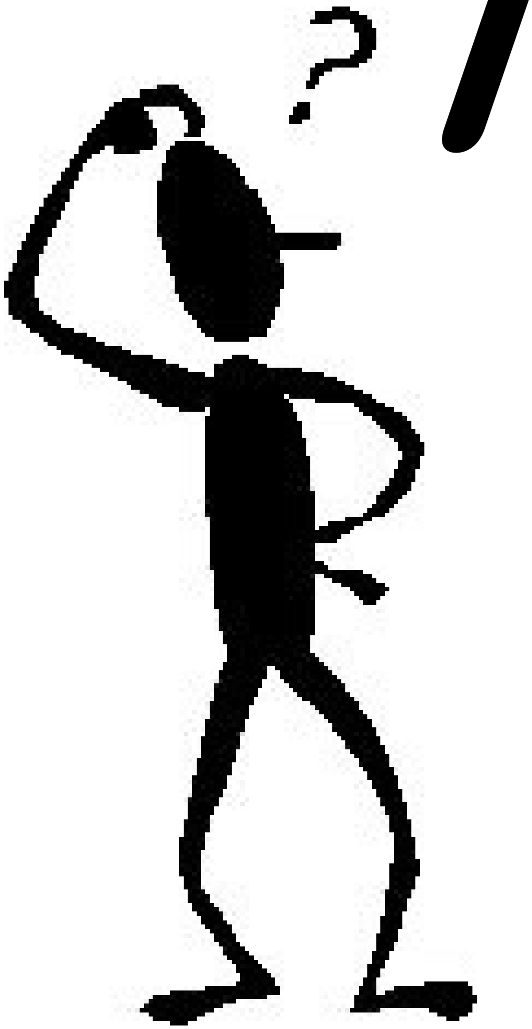
Agenda

- Overview
- The Purpose and The Proposal
- Possible content and topics
- For today: Determine some topics of general interest, and bounce those around

  …. to see if any magic occurs
- Where do we go from here?

Why “Tales from the War Room”??

- There’s lots of opportunities for technical discussions and how to respond to typical threats, technologies, etc.
- But very little chance to talk to others in the hot seat about *how to manage* an incident response group…. From a non-technical point of view.
  - What works for others (tools, methods)?
  - What challenges do you have?
  - How to manage Responders and the work they/we do?
- So this is an attempt to facilitate that kind of discussion, and see if we can all learn some new things and jointly benefit.
- If it’s valuable, then are there ways to do this continuously?



The Core

Now that I { have | am } a **CSIRT** group,
what do I do next?

THE CHALLENGE

- Few (if any) rehearsals
- No score
- No warnings
- All improvisation

THE AUDIENCE

- Impatient
- Demanding
- Anxious
- Thankful (hopefully)

THE PLAYERS

- Not necessarily ready, willing (or awake).
- May have not worked together before.
- Asked to do unusual things.
- Might have conflicts.

THE PERFORMANCE

- Likely won’t ever be repeated.
- Needs to be near-perfect, the first time.

OUR JOB

The Incident Response *management* TOOLBOX

- Is it empty?
- What kind of tools do you have? (or wish you had?)
- Do your tools allow you do perform effectively and efficiently?

- ✓ Incident Record-keeping
- ✓ Contacts
- ✓ Definitions
- ✓ Procedures
- ✓ Communications
- ✓ Statistics
- ✓ Reports
- ✓ Action Trackers

Topics for Consideration

- Case Management
- War Rooms
- CSIRT tools
- Communications
- Contacts Management
- CSIRT meetings
- After the Incident
- Care and Feeding of the CSIRT team.
- CSIRT futures.
- CSIRT Core- Where do we go from here?

Incident/Case Repository

- FIRST, Cert, Enisa, and others have material out there about what to do: http://www.first.org/resources/guides/csirt_case_classification.html
- And some of the tools that are available: http://www.enisa.europa.eu/act/cert/support/chiht/implementing-procedures/incident-tracking-reporting

What's "state of the art" and in widespread use? (everyone I talk to seems to be looking!)

Incident/Case Repository

January, 2010 threads on FIRST discussions:

–http://code.google.com/p/rapier/

–RT, RTIR, RTVIR - http://bestpractical.com/

–www.pyflag.net

–SIRIOS - http://www.otrs.com/en/

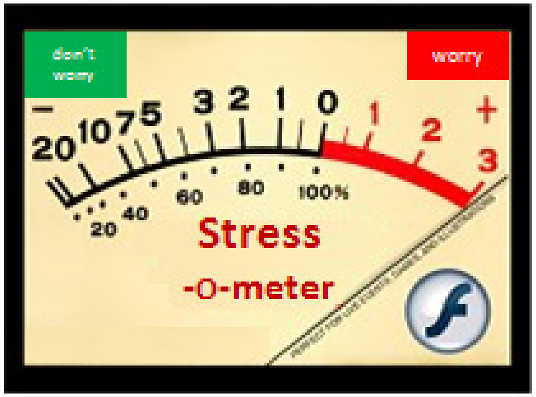
Notes from the Session:

- AIRT is another tool that should be considered.
- SIRIOS.org is the correct link to SIRIOS.
- Comments: many times, database systems are too restrictive, so we stick with file system storage.

- All seemed to be in agreement that a good Incident/Case Management System is difficult to find; most teams consider their current tool as "temporary" until something better comes along.

War Rooms

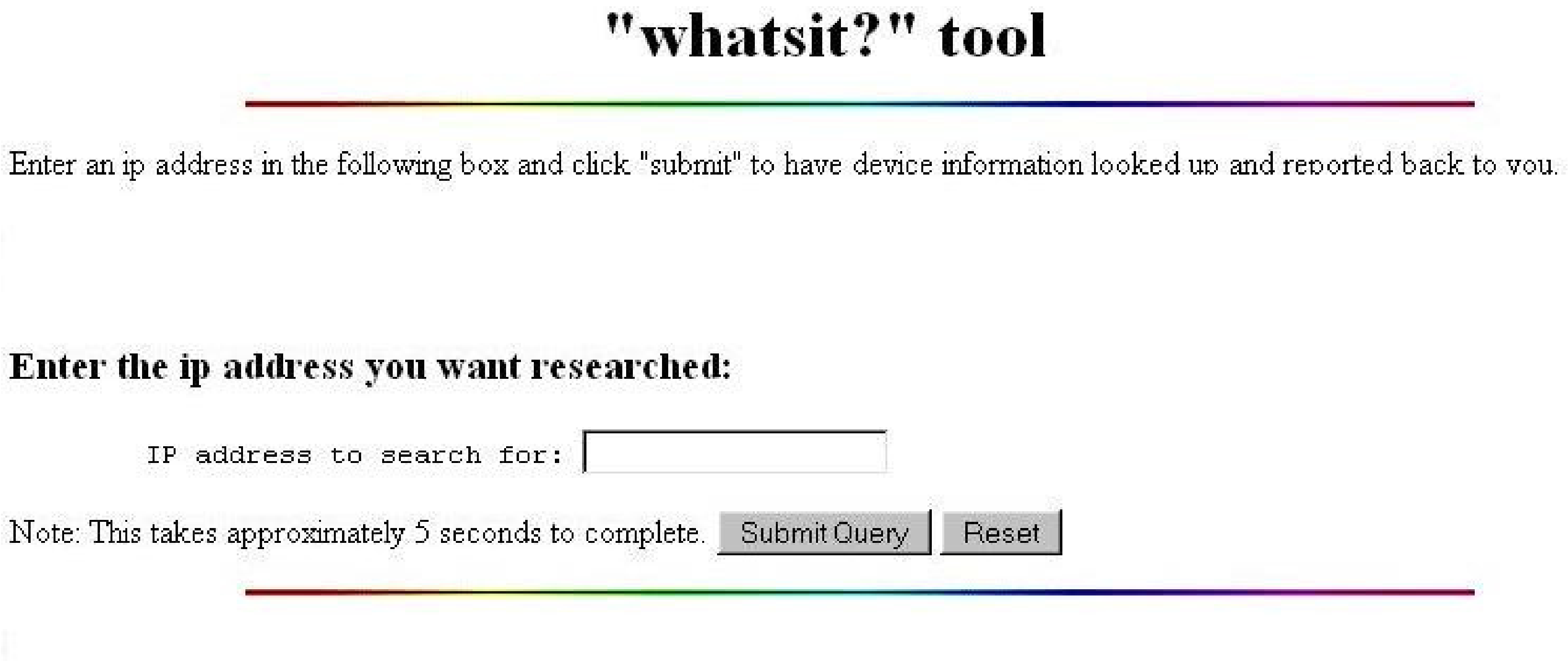
- How many have a War Room?
- What works…. And what doesn’t?
- When are they needed/recommended?
- Do you find a productivity loss when you drag stuff into the war room?
- How do you provision it?
    - Pc’s
    - Projectors
    - Other?
- Recommendations for others?



Notes from the Session:

- Why have a war room? The desired situation is a table where all the team members can see all the primary displays at the same time, 5 seconds from primary work areas. Use a bell to summon people to the room when needed.
- Questions from the floor: Why is 5 seconds important. Why not 10, 15, etc? Is there a "sweet spot"?
- Some discussion regarding efficiency and effectiveness balances. Taking a Responder away from their primary workspace can be counter-productive…. However there are benefits to taking people out of their normal environment for the duration of a short, focused meeting, because sometimes you need to have people together to discuss and make decisions. Timing is important because getting in and out is simple. Calling and adjourning is fast and easy.

Whatsit?



"whatsit?" tool

Enter an ip address in the following box and click "submit" to have device information looked up and reported back to you.

Enter the ip address you want researched:

IP address to search for:

Note: This takes approximately 5 seconds to complete.

Results returned:

```
Results of analysis:

***************************
*    WhatsIT?    *
**************************


BTW: you are coming from: 1.2.3.4

Lookup for ip address:          5.6.7.8,
   nslookup from dns #1 returned:         name1.something.com
   nslookup from dns #2 returned:         name2.something.else
   nbtstatus information shows:           (display of netbios
information, if available)

   5.6.7.8 is reachable via a ping.

   Location information found for ip address 5.6.7.8:


   Historical information found:
```

Under the covers:

Simple web page, calls a perl script via: <form method="get" action="/foo/bar/whatsit.pl">

```
use CGI::Carp qw(fatalsToBrowser);
# DNS  lookup
                $nslookup = "";
                open NSLOOKUP, "nslookup $ip 11.11.11.11 2>&1 |";
                while (<NSLOOKUP>) {
                                if ( my ($junk, $name)
                                                = $_ =~ /^(.*)\s+name = (.*)/ ) {
                print "    nslookup from dns #1 returned: \t$name \n";
                }
                }
                close NSLOOKUP;
# NBTstat lookup
    print "    nbtstatus information shows: \n";
    $nbtstat = "";
    open NBTSTAT, "nmblookup -A $ip |";
    $hostname = "";
    $groupname = "";
    while (<NBTSTAT>) {
      my $fixedline = CGI::escapeHTML($_);
      print "$fixedline" if /ACTIVE/;
      if ( my ($junk, $mac)
        = $_ =~ /^(.*)\s+MAC Address = (.*)/ ) {
        print "    MAC Address is: \t\t\t$mac\n" ;
      }
    }
# Ping the machine now
  my $p;
  use Net::Ping;
  $p = Net::Ping->new();
    print "    $ip is ";
    print "NOT " unless $p->ping($ip, 2);
    print "reachable via a ping.\n";
  $p->close();
  print "\n";
# Lookup the historical info
  print "    Historical information found: \n\t";
  print grep m/\Q$ip\E/, slurp "/foo/bar/history/history.log";
  print "\n";
```

(thanks to Perlmonks.org and others!)

Handler’s Log

- Example: CSIRT diary... a handler surfs to a page and types in a one-liner (eg: opened CSIRT 1234 re xxxx. Meeting at 11:00). It "knows" who that person is from a cookie (captures userid one time by a prompt; remembers thereafter), and doesn't let anybody in other than some specific people (make them enter a password one time, then remember forever via a cookie). Also capture date/time and ip address they came from.
- Put this at the end (or top?) of a flat file to record "diary notes".
- A second page (accessible only to the same group) refreshes automatically every 30 (?) seconds; you can leave a browser window open to watch what others are doing.
- Would be *very* helpful across multiple sites... even more so for those who have a Security Ops Centre doing triage 7x24.

Notes from the Session re "handler's log":

- It sounds like John is looking for a *Twitter* that can be used internally and securely!
- If anyone can point John to sample code that could be modified to perform this function, he'd happily share the results with others!

Needed: A Network "Gizmo"

- Collect and display information about hosts on our network…. Gracefully handling all of:
  - Static NAT addresses
  - VLANs
  - Load Director "service" addresses
  - Multiple DNS's
  - Multi-home machines.
  - IP aliases
  - Virtual machines behind a host machine.
  - Maintenance IP addresses (ILO, etc.)
  - Contacts, criticality, zones, applications, etc.
  - Machines with multiple hostnames (or dynamic host names in the case of clusters)
  - All the other network wrinkles that they can think of.

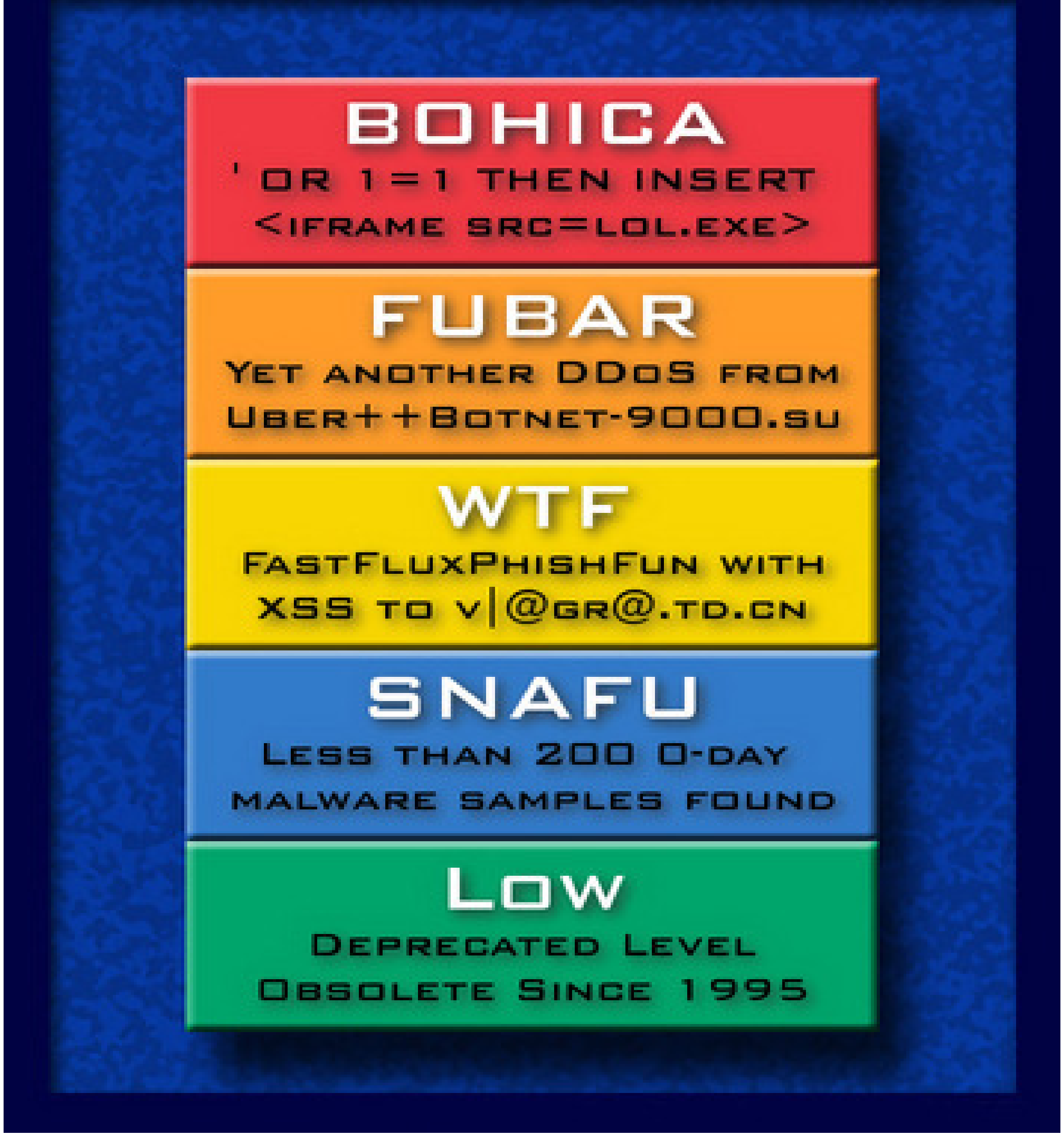
Notes from the Session re "network gizmo":

- Network Configuration information can be a challenge for many. Those who have tight change and asset management controls can leverage a resulting Configuration Management Database for CSIRT purposes…. Those without can struggle with triage, containment, and remediation. Incident Response should be a consumer of existing information and not have to reverse-engineer configurations during an Incident.
- Snort and Sourcefire was suggested as one method to determine empirically what is on a network and what types of systems they may be.

Notes from the Session: Other "wish list" items

- Log file parse tool, to identify IP addresses and targets. What has that IP address done, and when?
- More integrated tools that can collaborate in a meaningful way. More "glue" between applications to aid Incident Response.

Severities



BOHICA

' OR 1=1 THEN INSERT <IFRAME SRC=LOL.EXE>

FUBAR

Yet another DDoS from Uber++Botnet-9000.su

WTF

FastFluxPhishFun with XSS to v|@gr@.td.cn

SNAFU

Less than 200 0-day malware samples found

Low

Deprecated Level Obsolete Since 1995

CSIRT Severity Definitions

severity level		when this would be utilized	Incident Management- notifications and coverage	caveats and considerations
1	Severe; Major Security Incident	• impact to multiple businesses or services	• executive oversight required	• possible legislative, legal, or Business issues.
		• Extensive and visible service impact	• immediate notification to Executives. Daily status updates.	• possible financial costs resulting from the Incident and/or remediations (penalties, overtime, additional equipment, impact to projects, etc.)
2	High Alert; Incident Repose Team invoked	• increased focus by Management is desirable	• 7 x 18 continuing effort for remediation. Response being coordinated by CSIRT. Change Management may be bypassed.	• Post-incident review will be completed.
		• deteriorating or un-contained situation.		
3	Moderate; potential risks require focus	• a risk has been detected that requires ongoing monitoring or assessment.		• Post-incident review is optional.
		• further triage is necessary to ensure the nature of a risk is understood		
4	Low; Business as Usual	• researching potential threats or controls	• existing controls are sufficient to counter the threat.	
		• day-to-day security issues	• existing controls are sufficient to counter the threat.	• Post-incident review is not usually performed.

CSIRT Remediation Priorities

priority level		when this would be utilized	expected response	caveats and considerations
1	All Hands on Deck	• active attack that needs to be contained	• service disruptions may occur	
		• need to immediately terminate a service	• 7 x 24 continuing effort	• immediate notification to Executives
2	High Alert, Immediate Action	• urgent changes to security controls		• overtime costs may result
		• proactive infrastructure protection and preservation	• 7 x 18 (7 business days x 18 hours per day) staffing for remediation	• may affect project deliveries
		example: high-profile disclosure of a critical vulnerability that is expected to be attacked at any time.	• service disruptions are not expected in most cases, but any must be reviewed by CSIRT	
			• implementation targets are set by CSIRT.	
3	Heightened Awareness, priority action	• proactive infrastructure protection and preservation	• service disruptions are not expected	• immediate notification to Management in affected areas.
		• priority changes to security controls	• 5 X 18 continuing effort as appropriate to meet targets	
		example: high-priority attention to patches in a timeframe specified by CSIRT to counter a known threat that has no other compensatory controls.		
4	Business as Usual	• day-to-day security control maintenance	• normal patch cycles may be appropriate	• notifications for awareness; cases recorded for statistics
		example: updating a/v or IDS signatures; responding to routine virus detections	• service disruptions are not expected	

Definition: INCIDENT

An Incident is any situation where there is an actual or potential risk to our computer systems or a degradation of Computer Security controls or services that might affect us or our business that is not covered by "business as usual" processes.

When to open an incident:

- If in doubt, it’s an incident. The response process will determine specifics and risks.
- If immediate action is needed to research or correct a control failure or deficiency. If there’s a possibility of services being impacted by a security failure.
- If operational decisions are considering eroding security controls to restore service. If we need to take proactive measures to protect our systems or services.
- If there’s a possibility of legal action or public disclosure related to computer security controls.

Definition: EVENT vs. INCIDENT

Security Event

- Thousands per day.
- Business as usual is adequate to deal with it.
- Often handled by automation. (eg: AntiVirus quarantine, SPAM block)
- Aggregation of events may generate an alert to a potential larger issue.
- Risk is determined by automation or reporting.
- Primarily reported by statistics.

Security Incident

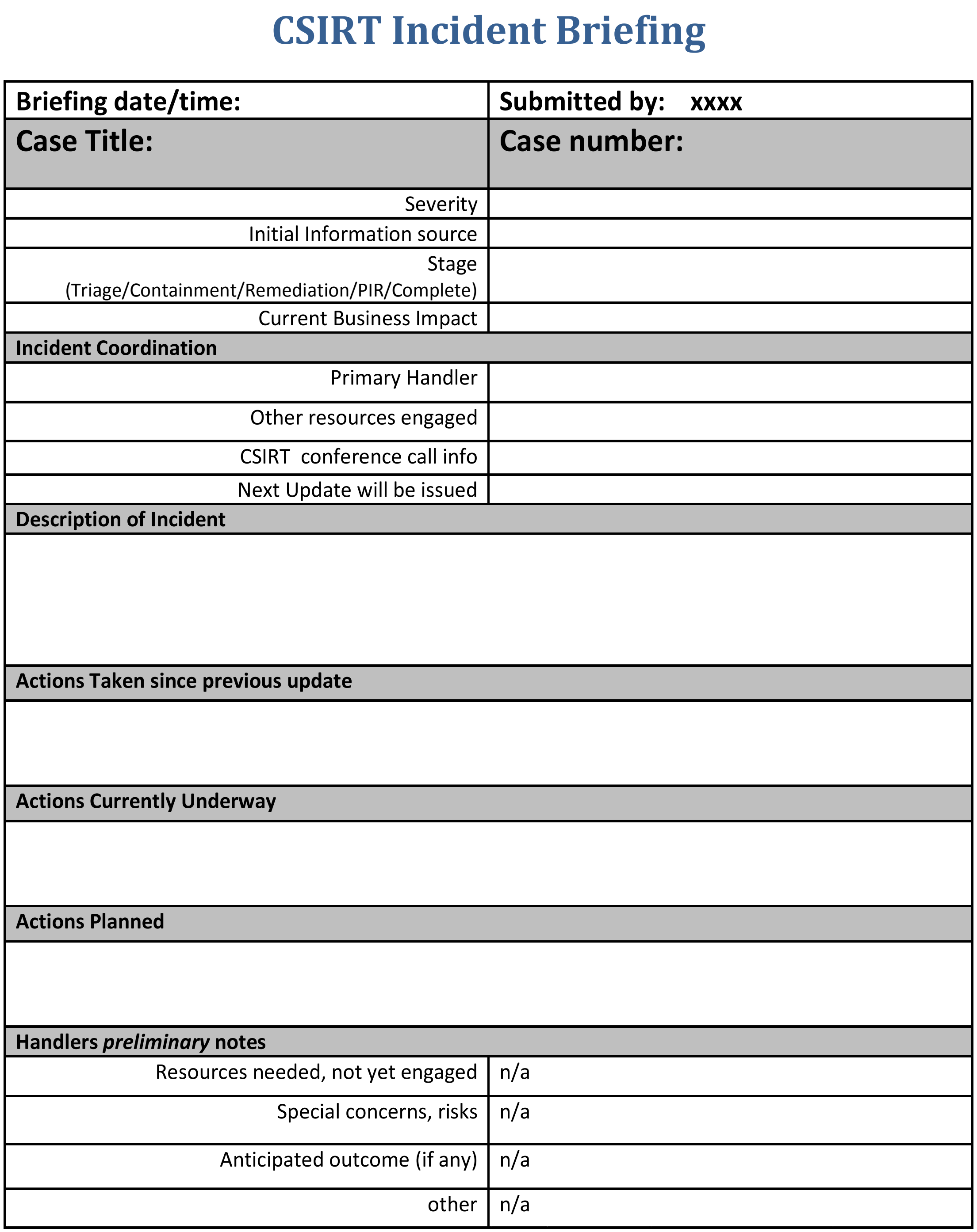
- Hopefully none!
- Cannot be handled by automation.
- Special attention is needed.
- More details are tracked.
- Subject Matter expertise is engaged to assess risk.
- Formal processes to determine severity and perform triage.
- Wider audience for notifications, typically.

CSIRT Communications

- Multiple types- Technical vs. Management vs. statistics.
- How to reach the right group of people to read your reports?
- How to communicate clearly & set expectations.
- How to prevent your material from becoming spam?

Briefing Document

- Standard look-and-feel.
- Handler fills this out, the pastes the contents into an email for easy viewing directly in a mail client (and on Blackberries).
- Also save the word.doc file in case records and for easy updating the next time.
- Sent to a standard mail list, *plus* other parties that have been engaged.
- The briefing document can be used for an initial notification (and while triage is ongoing), and allows for a quick **opinion** from the handler.
- Also have a similar, more detailed "Meeting Minutes" document, that includes specific names, departments, etc. In that one, we also identify the tactical remediations separately from the strategic remediations that will need to happen later.
- Note that we set expectations for when the audience should expect to hear more.



CSIRT Incident Briefing

Briefing date/time:	**Submitted by:** **xxxx**
Case Title:	**Case number:**
Severity	
Initial Information source	
Stage (Triage/Containment/Remediation/PIR/Complete)	
Current Business Impact	
Incident Coordination	
Primary Handler	
Other resources engaged	
CSIRT conference call info	
Next Update will be issued	
Description of Incident	
Actions Taken since previous update	
Actions Currently Underway	
Actions Planned	
Handlers *preliminary* notes	
Resources needed, not yet engaged	n/a
Special concerns, risks	n/a
Anticipated outcome (if any)	n/a
other	n/a

CSIRT Mail list Hierarchy

Guiding Principles

- Minimize the opportunities for Handlers to select an incorrect list
- Leverage other mail lists extensively, to move the maintenance accountability to other departments.
- include a generic mailbox that archives all email to all groups.

Contacts Management

Needed:

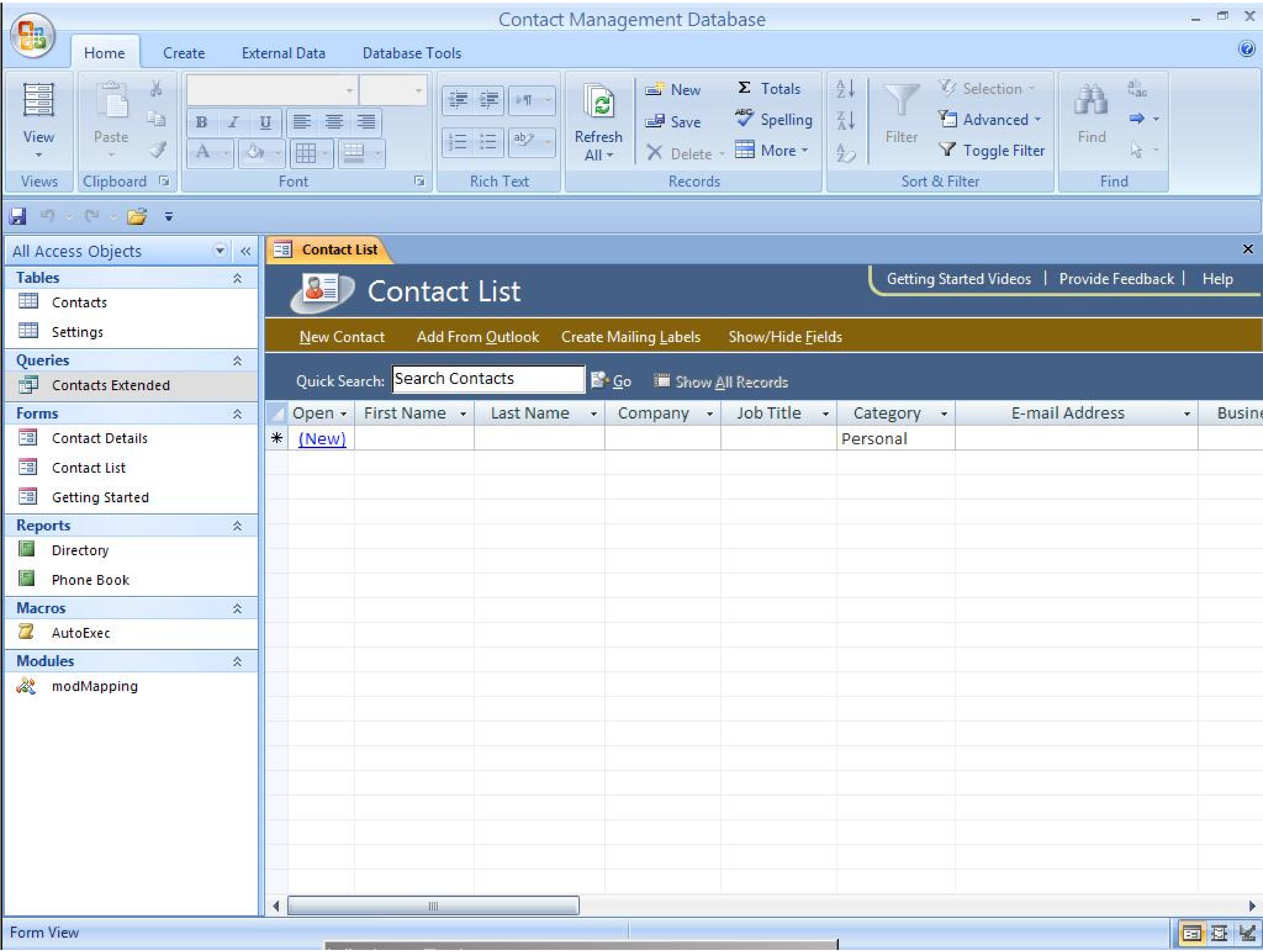
- A database that can relate contacts to groups.
- Email interface to generate attestation reviews and perform updates.
- Fields to record attestation dates.
- Interface to Active Directory to obtain information when available.
- Build and maintain mail lists for resulting groups.

Solutions:

- None known so far.
- MS Office Access (2007 and 2010 beta) have a “contacts” template that does much of this, except:
  - Can’t collect attestation dates
  - Can’t handle two tables (groups and contacts) and perform updates across both as needed.
  - Can’t maintain mail lists.

Notes from the Session: contact lists

- Some groups have been able to use LDAP successfully with a custom database schema to obtain lots of information to aid Incident Response.



Contact List

Quick Search: Search Contacts

	Open	First Name	Last Name	Company	Job Title	Category	E-mail Address	Busine
*	(New)					Personal		

Incident Meetings
(aka: herding the cats)

Incident Meetings
Some challenges

- 30+ people on a conference call.
- 36-hour long conference calls.
- 2 hour meeting- can take 2 hours to document
- Sending spreadsheets to a group; merging multiple edits into one “master” copy.
- Side conversation management
- Technical and executive staff on the same line.

Incident Meetings

--making sense out of chaos--

Incident Meetings
Some answers

- Divide the problem into parts and groups.
  - Assign a coordinator for each group.
  - Send each group off; report back in xx hours.
  - This also gets the techies on one call, away from the Executives.
- Assign someone to brief Executives.
  - Let them talk amongst themselves.
- Set expectations: “next briefing at xx:xx”

Incident Meetings
Some (more) answers

- Open a “technical” line for the duration
  - use a speaker phone!
  - let the techies conference in as needed.
  - They can yell if they need a Responder’s attention.
- Open a “management” line for specific meetings.
  - Set a time limit, try to stick to it.
  - Don’t consume your Experts in explaining things. (that’s why we have middle-Management)

Incident Meetings
Meeting minutes

- Assign a senior Responder to manage “the process”.
- Assign a junior to be the scribe.
- Type notes in real-time, preferably in a chat window, where meeting members can notice and correct errors on the fly.
- Collect email addresses to be included for distribution in a wordpad document. Hand that document off to the next shift for maintenance.
- Have a cheat sheet -things to think about- that Responders can check off.

Notes from the Session: incident meetings

- Google WAVE was suggested as one tool that might be of interest…. But with privacy issues that need to be considered!
- Re “real time meeting notes”- rather than re-wording these and publishing as minutes, consider the raw notes entered on an IM application to be the “minutes”.
- Discussion re Public Relations and dealing with The Press- this is a big issue for most Responders and needs to be facilitated as part of many Incidents.

After the Incident

- "Those who do not learn from history are doomed to repeat it.“ (George Santayana)

- “Any lesson you learn as the result of a Security Incident is a *very expensive* lesson to learn. You don’t want to learn it a second time.“ (someone in FIRST)

Post Incident Reviews

- We use them to:
  1. Identify root cause, contributory factors, and strategic mitigation that is required.
  2. Review how well the CSIRT process itself worked and if there are opportunities to improve it.

- Can be a delicate subject.. So we take pains to reassure those involved that we do not assign blame, but identify control deficiencies that allowed the incident to occur.
- Control deficiencies could be technical, procedural, organizational.
- We also separate mitigation actions into tactical (during the incident) and strategic (to be fixed later).

Post Incident Reviews

- A challenge: how do organizations ensure that strategic mitigation is actually done (before we're doomed to repeat the past)?
- One of my goals is to "document and get out".
  - There might be another Incident that needs us.
  - Control design and implementation is fair game for Responders to critique, but if we are further involved in solutioning, then we lose our independence.
- What works for you?

Root Cause

- Needed: a good definition of root cause.
- Depending upon the individual doing the assessment, how busy they are, and their interest in the subject… you can get quite different answers.

- Suggestions on how to standardize?

Security Metrics

This topic alone could take the rest of the day, and can often deteriorate into extended (and heated) discussions. There are lots of resources out there for this; I suggest we defer to those other resources.

- Dan Geer "Measuring Security" *recommended*
  - google for "measuringsecurity.tutorial.pdf"
- SecurityMetrics.org
  - Metricon 4.5 coming up, March 1, 2010. Lots of prior art out there (See above).
  - Active mail list you can subscribe to.
- FIRST Metrics Special Interest Group
  - https://amnesia.first.org/pages/listpages-dirview.action?key=metricssig
- Argonne National Laboratory – Physical Security Maxims
  - http://www.ne.anl.gov/capabilities/vat/pdfs/security_maxims.pdf
- A Framework Based On Continuous Security Monitoring
  - http://www.sat.metu.edu.tr/private/volkanerturk/CSM_thesis.pdf

Sample posting (Jan 7, 2010) from SecurityMetrics mail list

1.Economics of “perverse incentives” and unintended consequences:

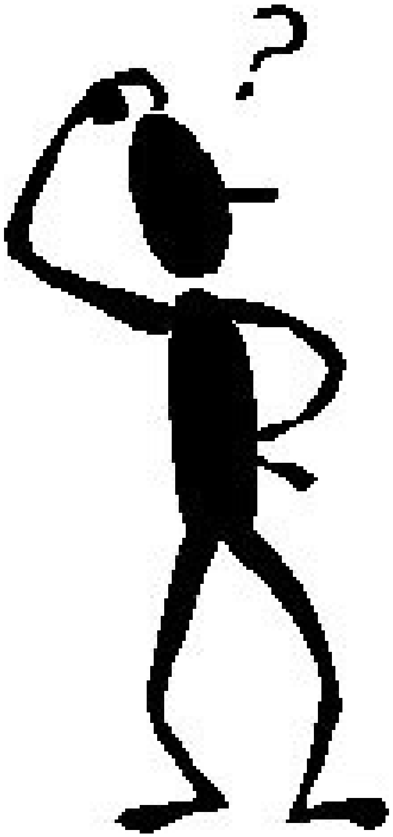
http://en.wikipedia.org/wiki/Perverse_Incentives
http://sifaps.egc.ufsc.br/index.php?option=com_docman&task=doc_download&gid=36&Itemid=38
http://articles.techrepublic.com.com/5100-10878_11-5887819.html
http://www.econlib.org/library/Enc/UnintendedConsequences.html
http://www.marginalrevolution.com/marginalrevolution/2008/01/the-law-of-unin.html

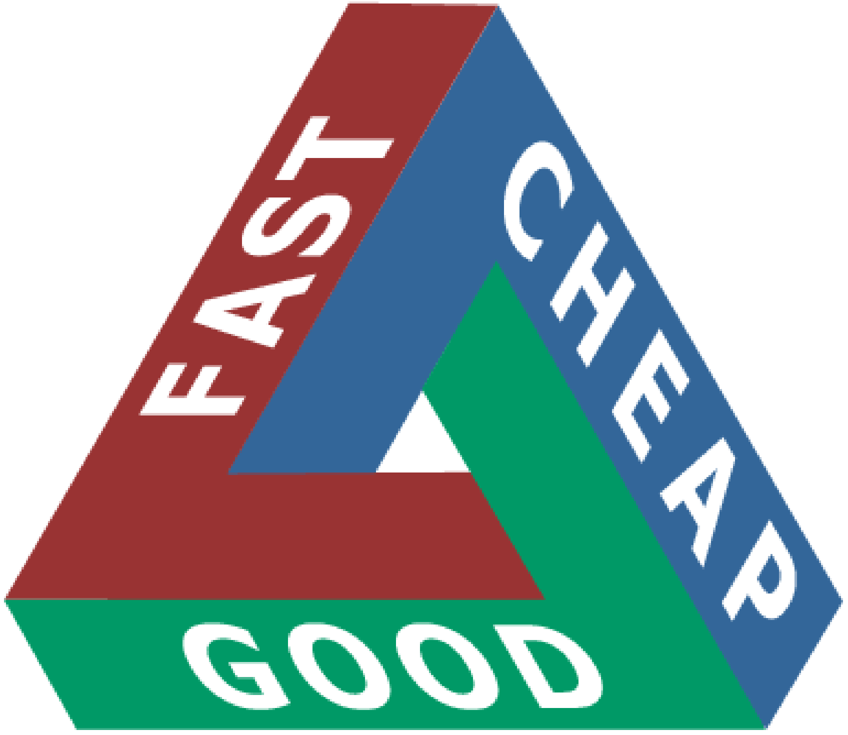
2. System dynamics archetypes, especially “Drifting Goals”, “Fixes that Fail”, and “Shifting the Burden”.
See: http://www.b-eye-network.com/view/8469

3. Self-defeating organizations:
http://www.amazon.com/Self-Defeating-Organization-Companies-Outsmarting-Themselves/dp/0201483130
http://www.turnaround.org/Publications/Articles.aspx?objectID=788

4. Reverse or Anti-Hawthorne effect (if the act of being measured results in reduced performance, rather than the value of the metrics as a signal)
http://blogs.isixsigma.com/archive/the_anti_hawthorne_effect.html

Managing:
"The Core"





CSIRT Team *Creation*

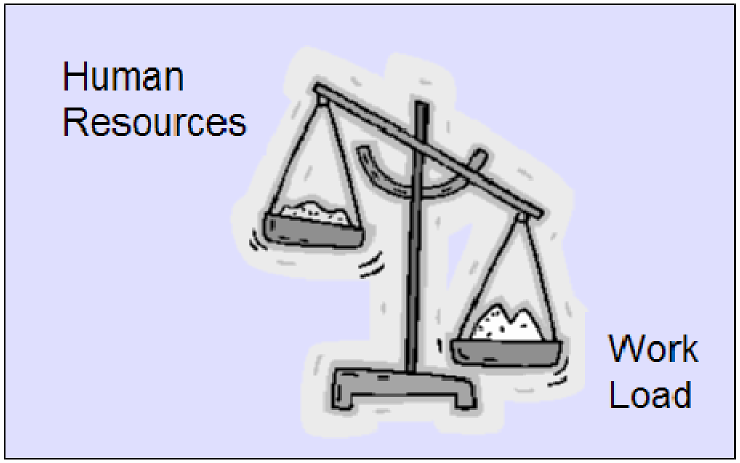
- http://www.cert.org
- Enisa
- FIRST
- Team constituencies, size, scope, and degree of technical involvement vary widely.
- Lots of resources and references available.

CSIRT Team *Maintenance*

- Where can we (Responders or Leaders of Responders) learn about how to:
  - Manage staff under stress?
  - Recognize and prevent burnouts
  - Effectively rotate shift coverage in an emergency
  - Shield our staff from interruptions
  - Focus responders to manage the response, not solution it.
  - Recognize and reward the excellence that we're hoping to receive.
- Training- one source- PStephen@Norwich.edu
  - www: drstephenson.pbworks.com
- http://www.enisa.europa.eu/act/cert/support/exercise

Limits to Effectiveness in Computer Security Incident Response Teams

- http://www.cert.org/archive/pdf/Limits-to-CSIRT-Effectiveness.pdf
- Great paper on CERT organizations and maintaining them over time. For example:
  - Common problems among CSIRTs
  - Working Smarter: Investing in Automation



Was this useful?

- Feedback is welcome – to CSIRT.core@gmail.com
- Or to me personally, of course.
- What would you do differently? More of? Less of?
- Should we find ways to do more of this on an ongoing basis?
- If so, then I have the following suggestions:
  - Set up a wiki for CSIRT Responders/Managers to talk about *our trade, toolboxes, and techniques.* First has one we might use…. How many are / are not First members? Or externally?
  - Set up a mail list? Any volunteers?
- If useful and we carry on with collecting and sharing information, then I'll volunteer to facilitate a session in Miami in June.
- I'd like this to turn into a Special Interest Group (or Birds of a Feather session) that can meet regularly, whenever there is a FIRST (or TF-CSIRT) session.
- Another brewery trip might be a good venue, no?

Questions?

or via email to:

CSIRT.core@gmail.com

TALES FROM THE WAR ROOM VERSION 1.0

FIRST Annual Conference

Miami, USA

June, 2010

→ To be continued? ←