



CISSPworld

[Home](#) · [Calendar](#) · [Classifieds](#) · [Careers](#) · [Downloads](#) · [Your Account](#) · [Forums](#) · [Logout](#)

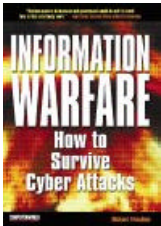
Search

### Big Story of Today

Today's most read Story is:

[Surrender Dorothy!](#)

### Recommendations @ Amazon



### Buy Item From:



[Support CISSPworld](#)

### Public Access

- [Home](#)
- [FAQ](#)
- [Career Centre](#)
- [Search](#)
- [Stories Archive](#)
- [Submit News](#)
- [Surveys](#)
- [Recommend Us](#)
- [Feedback](#)
- [Key Server BETA](#)

### Members Only

- [Classifieds](#)
- [Columnists](#)
- [Downloads](#)
- [Events Calendar](#)
- [Forums](#)
- [Members List](#)
- [Net Query](#)
- [Newsletter](#)
- [Private Msgs](#)
- [Reviews](#)
- [Seti@Home](#)

## Surrender Dorothy!

Posted on Tuesday, December 03 @ 00:05:00 GMT by [manager](#)



In his first CISSPworld column Adam Pressman, CISSP, provides us with a security management article and says "So much time and money is spent trying to predict the bad things that can happen in network traffic. It's a never ending struggle. A paradigm shift in thinking about network control is required. Lets learn what SHOULD be on our networks and allow only that."



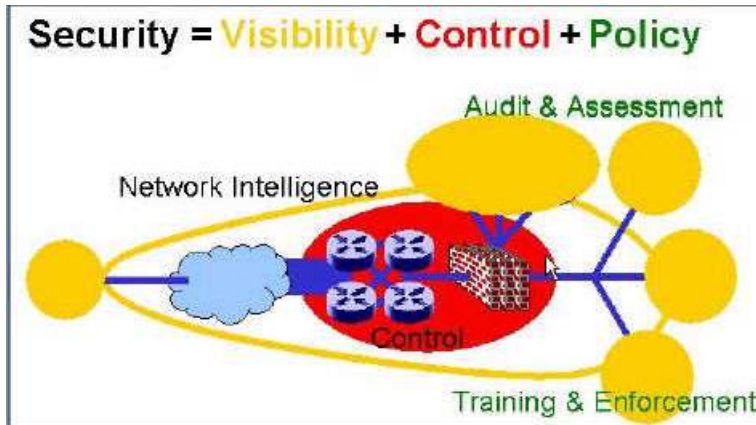
Most network security philosophy is oriented around the concept of predicting the bad things that can happen to a network. Excluding those should mean everything else the network is doing, presumably, is valued. Predicting all the bad things that CAN happen is an unattainable goal. Surrender! Give up! You can't win at this.

Why presume?! Why do we not KNOW what the valued work requires of the networks we build and manage? Because it changes all the time. That's not enough of an excuse from knowing however. What are you going to tell the Chief Information / Executive Officer (She / He is the distinguished looking one who owns the network) in that 2 minute elevator ride when she / he asks you...

### What's on my network?

Unless you have prepared a periodic review of what the users (Yes... talk to the users) expect of the network and a less periodic analysis of what's really happening on your network, you can't predict the valued traffic of your network. And boy howdy, if you could isolate what makes valued traffic, your job is real easy to understand. Everything else you exclude. Easy huh!

Okay... here's the practice. Instead of spending every moment of your security workday looking at the logs for something that shouldn't be there, downloading every intrusion detection signature and patch that comes along, interview your users. Bring an effective network visibility tool. Show the network owners what is going on. Define what the two of you are seeing. Ask, is this supposed to be here? If yes, add it to the availability checklist. If no, assure him that with your network control devices you promise: It can't happen here.



**Network Intelligence** - This can be network sniffer nodes, packet capture utilities or intrusion detection systems. The latter are the easiest to interpret and sift out the spurious network maintenance traffic you'll otherwise see. Not

### Login

CISSP Number

Password

Login

### This site is for CISSPs Only.

CISSP? Not registered?

[Create account now](#)

Registered users can access a whole range of additional services and resources.

### This site is for CISSPs only.

### Related Links

- [PHP HomePage](#)
- [Intel](#)
- [CISSPworld FAQ](#)
- [CISSPworld](#)
- [New Membership Application](#)
- [More about CISSPworld Content](#)
- [News by manager](#)

### Most read story about CISSPworld Content:

[Why become a CISSP?](#)

### Article Rating

Average Score: **3**  
Votes: **1**



Please take a

- [Stories Archive](#)
- [Topics](#)
- [Web Chat](#)
- [Web Links](#)
- [Your Account](#)

**Contribute**

- [Submit News](#)
- [Add Download](#)
- [Add Event](#)
- [Add Review](#)
- [Add Web Link](#)

**Old Articles**

**Thursday, November 28**

- [Snoopers, crackable keys hamper wireless LAN uptake](#) (0)
- [DPA workstation quizzes smart card safety](#) (0)
- [Linux unsafe in any network, analyst firm proclaims](#) (0)
- [China accused of jailing net users](#) (0)
- [TechWeb: Security hole affects RealPlayers](#) (0)
- [Experts warn Winevar worm is spreading](#) (0)
- [Hamas urging 'electronic Jihad', says Jewish group](#) (0)
- [First hackers sighted in high speed mobile phone arena](#) (0)
- [SMS security risks highlighted by Friends Reunited hacking case](#) (0)

**Wednesday, November 27**

- [Novel crackdown on file-sharing](#) (0)
- [Experts warn of buffer overflow flaw in Solaris](#) (0)
- [Would bandwidth caps slow swaps?](#) (0)
- [Three steps to safer SQL](#) (0)
- [New credit cards dangle from keychains](#)

all of what an IDS manufacturer says is malicious applies to your network. These are called false positives. False negatives mean your system is missing events that it should be reporting as positives. (Just because no one was in the forest to hear the tree fall doesn't mean it didn't make a hell of a noise!) You must review all of what's happening on the network with the people who use the network. Is it supposed to be happening? The important thing is to classify your network traffic with the people who pay for it. Do this often in periodic meetings..

- **Valued Traffic** - That which the customer specifically determines should be traversing the network. You'll have to explain what the protocols mean, but then he can tell you if they need that for his work.
- **Incorrect traffic** - This is the easy stuff, best blocked at your routers and firewalls. This is the wrong addresses for a given side of the network, Internet garbage, maintenance protocols, runt packets, and other traffic not supposed to be occurring.
- **Irregular traffic** - This is tougher. Correct user addresses are correctly using the network. User Jane is supposed to be able to email users on the Internet. Is she supposed to be sending them company secrets? Here's where constant diligence in meeting with your user community will pay off in expanded salaries and security budgets. Meeting with the user management to learn what should be occurring is the first step. You then adjust your control devices and system to exclude everything else. Lastly you educate the user community with WHY the valued traffic is valued and that anything else they do will be blocked or logged. Also educate them on why this helps them too. Security is good.

**Control** - These are your firewalls, routers, content screening hosts or appliances that can remove the traffic you don't want.

**Policy** - Like good health, you can't buy security. It's a practice not a part number. Also like good health it takes thoughtful purchases, money for insurance but most importantly, an investment in time. If you don't have a policy, I've included some good links and suggested reading here on my site. And I offer to join you in a continued dialogue if you wish. The most important thing is to train your users. Note the smart rancher who learned that if the fence falls down nurtured cows don't leave. If the users understand and embrace the need to avoid pornography browsing (at least at work) they won't do it, even if your web content filter host fails. Educate, educate and when you're done educating, do some teaching. Make sure all who are responsible for security on your network appreciate how important their own contribution can be.

**Adam Pressman**

If you would like to write for CISSPworld then please email [manager@cisspworld.com](mailto:manager@cisspworld.com)

second and vote for this article:

- ★★★★★
- ★★★★☆
- ★★★☆☆
- ★★☆☆☆
- ★☆☆☆☆

[Cast my Vote!](#)

**Options**

- [Printer Friendly Page](#)
- [Send to a Friend](#)

"Login" | [Login/Create an Account](#) | 0 comments

Threshold  Thread  Oldest First  [Refresh](#)

The comments are owned by the poster. We aren't responsible for their content.

(0)

- [Risk of internet collapse rising](#)  
(0)

**Tuesday,  
November 26**

- [Computer viruses face slow down](#) (0)
- [Fraud fears still hamper online sales](#) (0)
- [DDOS attack 'really, really tested' UltraDNS](#) (0)
- [Webcast: Advanced IDS with Ed Yakabovicz \(CISSP\)](#) (0)

**Monday,  
November 25**

- [Viruses still costing businesses](#) (0)
- [Bond's Q: DVD will self-destruct in 36 hours](#) (0)
- [The spy inside your home computer](#) (0)
- [Bootleg probe targets cadet computers](#) (0)
- [Bush signs landmark security act](#) (0)
- [Lawyers Fear Misuse of Cyber Murder Law](#) (0)
- [Baker & McKenzie Global E-Law Alert](#) (0)
- [Merde! Alcatel LAN switch ships with backdoor access](#) (0)
- [Internet Performed Well During 9/11 Attacks - Report](#) (0)
- [Security Firms See Long-Awaited Windfall](#) (0)
- [Pentagon drops Internet ID plan](#) (0)

**Sunday,  
November 24**

- [Efforts to stop music piracy 'pointless'](#) (0)

**Friday,  
November 22**

- [Report: Net, e-commerce boom continues](#) (0)
- [CERT® Advisory](#)

- (0)
- [Efforts to stop music piracy 'pointless'](#) (0)
- [Net activism offers lessons for ministers](#) (0)
- [On the Microsoft FTP server leak](#) (0)
- [Worst Practices in Customer Privacy Management](#) (0)
- [ISC seeks cash amid BIND security concerns](#) (0)
- [Webcast: Is public instant messaging safe?](#) (0)
- [New User Competition](#) (0)

#### **Older Articles**

All information and content copyright the CISSPworld project. This site is created under license from (ISC)2.  
For any questions please email [manager@cisspworld.com](mailto:manager@cisspworld.com)

CISSP® is a registered certification mark and (ISC)2 is a service mark of the International Information Systems Security Certification Consortium, Inc . Their use is licensed and all rights are reserved by (ISC)2.