

THE ERA OF DESTRUCTIVE ATTACKS

ARE YOU PREPARED?

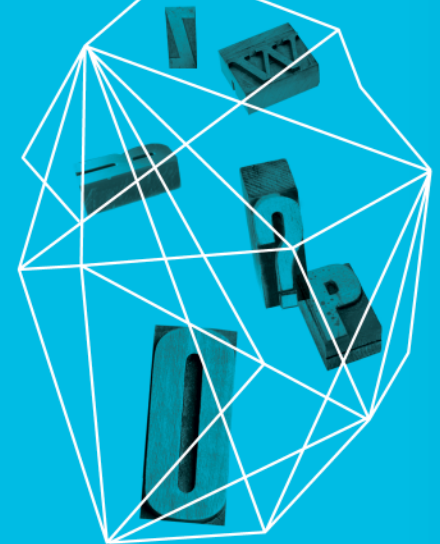
Erik de Jong

FoxCERT by Fox-IT

Frank Incognito

FoxCERT by Fox-IT

Security in
knowledge



RSACONFERENCE
EUROPE 2013

— Intro / agenda

- ▶ About us
- ▶ What is destructive, and how likely is that?
- ▶ A major cyber crisis – what will happen?
- ▶ How to prepare?



FOX IT

800-FOXIT

WHO YOU GONNA CALL?



Work by Srikanth Jandhvala @Flickr



Work by Rolf Bostedt @ Flickr





— What is destructive?






Ownage

Total ownage

Destruction



How likely is it?

					
Total ownage	likely	maybe	maybe	likely	likely
Destruction	maybe	unlikely	maybe	maybe	likely





Door ANGELOUX @ Flickr

— What will we talk about?

1. Detection
2. Interpretation
3. Escalation
4. Crisis mode
5. Business
6. Investigation
7. Communication
8. Legal
9. Back to “business as usual”

Detection



Interpretation



Door Phillie Casablanca @ Flickr

Escalation



Crisis Mode



Business



Investigation



Communication



Legal

1. DEFINITIONS - These definitions shall govern:

- A. "DRI" means DIGITAL RESEARCH INC., P.O. Box 579, Pacific Grove, California 93950, the author and owner of the copyright on this SOFTWARE.
- B. "CUSTOMER" means the individual purchaser and the company CUSTOMER works for, if the company paid for this SOFTWARE.
- C. "COMPUTER" is the single micro-computer on which CUSTOMER uses this program. Multiple CPU systems may require supplementary licenses.
- D. "SOFTWARE" is the set of computer programs in this package, regardless of the form in which CUSTOMER may subsequently use it, and regardless of any modification which CUSTOMER may make to it.
- E. "LICENSE" means this Agreement and the rights and obligations which it creates under the United States Copyright Law and California laws.

2. LICENSE

DRI grants CUSTOMER the right to use this serialized copy of the SOFTWARE on a single COMPUTER at a single location so long as CUSTOMER complies with the terms of the LICENSE, and either destroys or returns the SOFTWARE when CUSTOMER no longer has this right. CUSTOMER may not transfer the program electronically from one computer to another over a network. DRI shall have the right to terminate this license if CUSTOMER violates any of its provisions. CUSTOMER owns the diskette(s) purchased, but under the Copyright Law DRI continues to own the SOFTWARE recorded on it and all copies of it. CUSTOMER agrees to make no more than five (5)

copies of the SOFTWARE for backup purposes and to place a label on the outside of each backup diskette showing the serial number, program name, version number and the DRI copyright and trademark notices in the same form as the original copy. CUSTOMER agrees to pay for licenses for additional user copies of the SOFTWARE if CUSTOMER intends to or does use it on more than one COMPUTER. If the micro-computer on which CUSTOMER uses the SOFTWARE is a multi-user microcomputer system, then the license covers all users on that single system, without further license payments, only if the SOFTWARE was registered for that microcomputer. This is NOT a license to use the SOFTWARE on main-frames or emulators.

3. TRANSFER OR REPRODUCTION

CUSTOMER understands that unauthorized reproduction of copies of the SOFTWARE and/or unauthorized transfer of any copy may be a serious crime, as well as subjecting a CUSTOMER to damages and attorney fees. CUSTOMER may not transfer any copy of the SOFTWARE to another person unless CUSTOMER transfers all copies, including the original, and advises DRI of the name and address of that person, who must sign a copy of the registration card, pay the then current transfer fee, and agree to the terms of this LICENSE in order to use the SOFTWARE. DRI will provide additional copies of the card and LICENSE upon request. DRI has the right to terminate the LICENSE, to trace serial numbers, and to take legal action if these conditions are violated.

4. ADAPTATIONS AND MODIFICATIONS

CUSTOMER owns any adaptations or modifications which CUSTOMER may make to this SOFTWARE, but in the event the LICENSE is terminated CUSTOMER may not use any part of the SOFTWARE pro

Back to “Business as Usual”

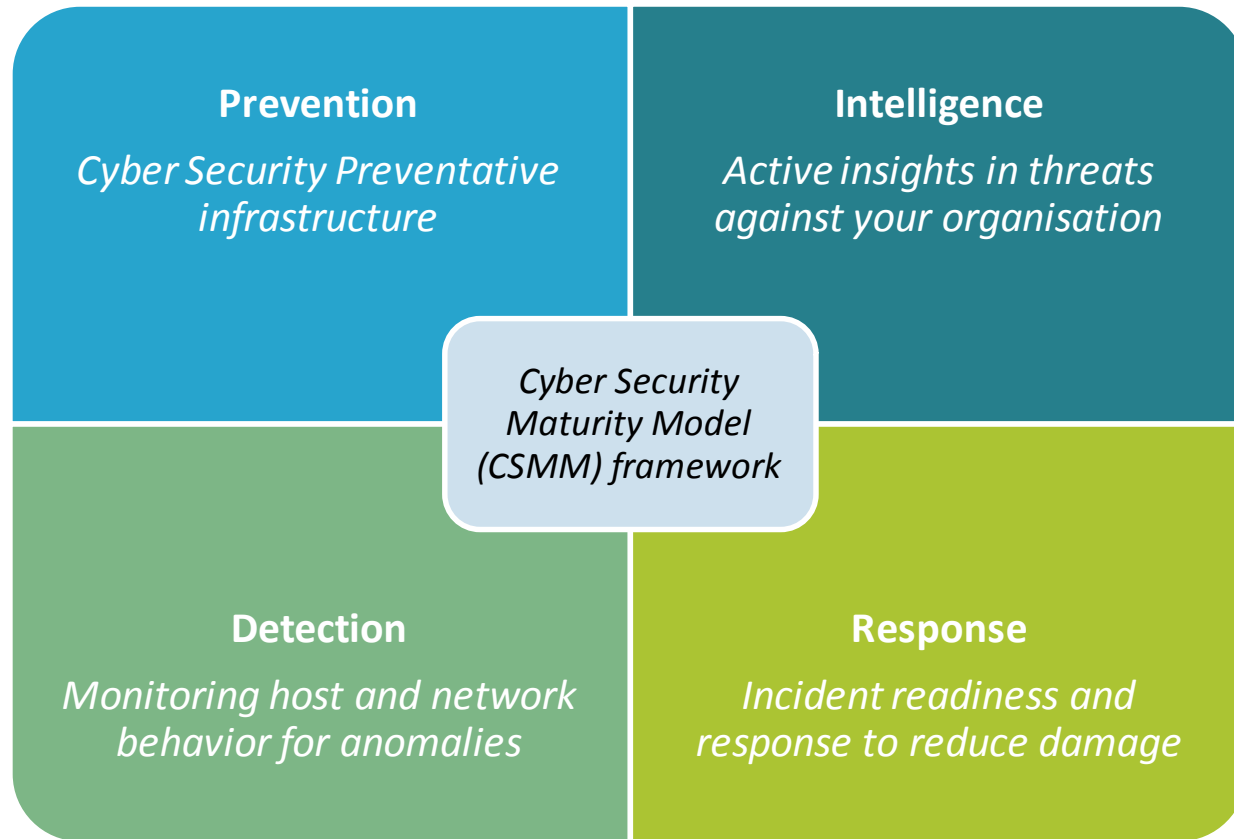


— How to prepare?

- ▶ Spend your money wisely
- ▶ Prevention
- ▶ Detection
- ▶ Intelligence
- ▶ Response

Spend your money wisely...

... assume you are owned



— Prevention

- ▶ Prevention *will* fail against certain actors
- ▶ Most organisations live in the 90s
 - ▶ Firewalls, AV, perimeter defense
- ▶ True resilience is expensive
 - ▶ True segmentation, not everything connected
- ▶ Be aware of weak spots (looking at you, marketing)

Detection

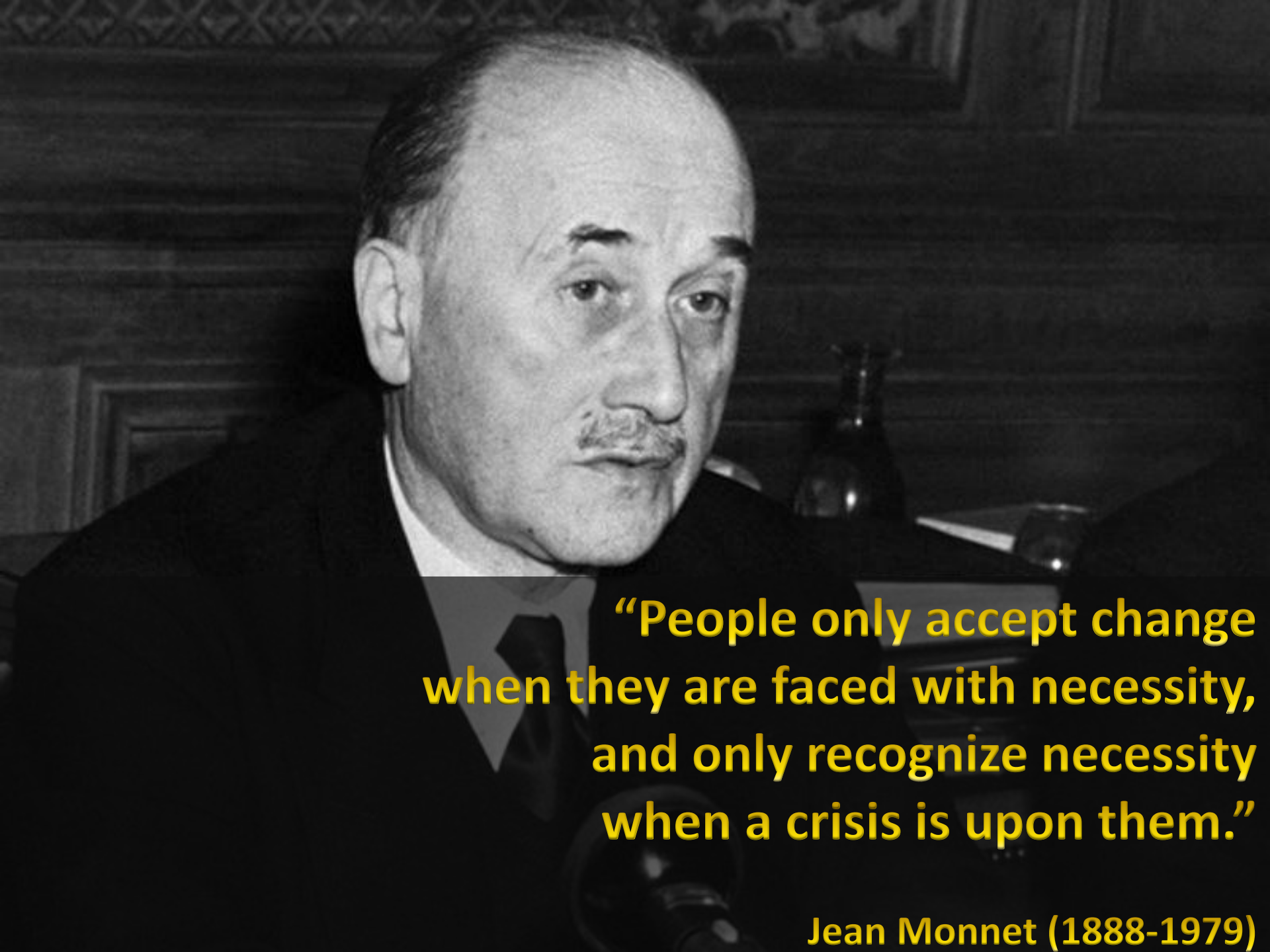
- ▶ Our experience: currently almost non-existent
- ▶ Looking back, there were always 16 ways to detect an incident
- ▶ Active vs. Passive?
- ▶ Outsourcing vs. doing it inhouse?
 - ▶ May need help with small investigations anyway
 - ▶ 3rd party will have wider scope and know more
 - ▶ True outsourcing doesn't exist
- ▶ What do you look at?
 - ▶ Everything? Crown jewels? Administrators?

— Intelligence

- ▶ Who's talking about you “out there”?
- ▶ Which information is already public?
 - ▶ Stolen credentials (not targeted)
 - ▶ Unintended leaks
- ▶ Use this information to help you
 - ▶ Reduce your vulnerability
 - ▶ Understand incidents

— Response

- ▶ Crisis plan
 - ▶ Who, what, where and **how**
 - ▶ Contact details
 - ▶ Process
 - ▶ Important information, projects, customers, systems
- ▶ Practice!
- ▶ Contract a 3rd party for incident response
 - ▶ Can you trust them? Where are they from?
- ▶ Forensic readiness
- ▶ Can you work offline? Backup plan?



“People only accept change when they are faced with necessity, and only recognize necessity when a crisis is upon them.”

Jean Monnet (1888-1979)

Thank you!

Erik de Jong

FoxCERT by Fox-IT

erik.dejong@fox-it.com

www.foxcert.com

Frank Incognito

FoxCERT by Fox-IT



RSAC CONFERENCE
EUROPE 2013