

When you Don't Know What you Don't Know

Business Risk Intelligence



Cyber threat Awareness

Le strategie di protezione tra cyber crime e sicurezza fisica nelle banche e nei settori più a rischio



BANCHE E SICUREZZA 2015



What Do

These All Have

In Common?

Each one has been
breached and their
customer data stolen
in 2014...





Altegrity

KROLL Background Screening



And in 2015.....



- Anthem
- Auburn University
- CareFirst
- Costa Coffee Club
- FireKeepers Casino
- InterContinental Hotel Group IHG
- Hard Rock Hotel & Casino
- Lufthansa
- Penn State University
- Premera Blue Cross
- Ryanair Airline
- Seton Family of Hospitals
- Starbucks
- University of California (UC) Riverside
- Etc. etc.



What Did
They All Have
In Common?

**No-one Had a
Clue What Hit
Them**



Amongst them Some of the Largest Companies in the World

Despite Each Having Spent
Millions on All The “Best”
Security Products, Software &
Consultants

Why Not?

Carbanak Attack (30+ Banks)

Sony

Anthem

Home Depot

Apple iCloud

UPS Boeing

JP Morgan

eBay

US healthcare.gov

US State Department

Carbanak Attack

Targeted attack that aims for financial profit rather than the typical stealing of enterprise's "crown jewels" or confidential data.

According to news reports, a backdoor hit more than 100 banks and financial organizations. The attack, which began late 2013, affected banks across the globe. Carbanak gang stole \$1bn.

Anunak?

- Entry vector – Phishing email with a CPL attachment**
- Basic Fail – No need for CPLs in email**
- Simple fix – whitelist attachments**
- Malware on ATM's, VPN over Network**
- Every bank should know and recognize traces of Carbanak infection**

Sony

Hacked at least three times – *Will they EVER learn?????????*

Last one (The Interview) \$40,000,000.00

Entry method – spearphishing with infected PDF to Admins

Basic Defence fail – Adobe Acrobat Installed

Simple solution #1 – any other PDF reader that does not allow running of executables

Simple solution #2 – print to PDF

Steal Admin password with malware

Simple solution - Multi-factor Authentication

Home Depot

Damage \$62,000,000.00

Stolen password from IT supplier (Airco)

Old vulnerability in Windows

Malware on POS (Check-out lanes)

Various Black POS, very old Windows XP malware

The RAM driver used in similar attacks 2005-7 by soupnazi

Basic Defence Fail: supplier LAN access

Basic Defence Fail: Single factor Auth

Basic Defence Fail: Antique OS

Basic Defence Fail: Static C&C Servers not detected via SIEM

...

Currently Being Sued

JP Morgan

>83 million of Personally Identifiable Information (Customer names, encrypted passwords, e-mails, registered addresses, phone numbers, Date of birth,....) from customers and small businesses got stolen

Attack Vector:

Old Vulnerabilities

Social Engineering/Phishing

Unattended and misconfigured Server

Network IDS's were not able to detect their presence

Attack only got noticed when a related (charity) site was also attacked

There is a pattern here.....

Exploits using old vulnerabilities

Phishing via e-mail or drive-by exploits

Attacks via Supply chain

Broken Technology

Non-detection of known malware by Anti-Virus

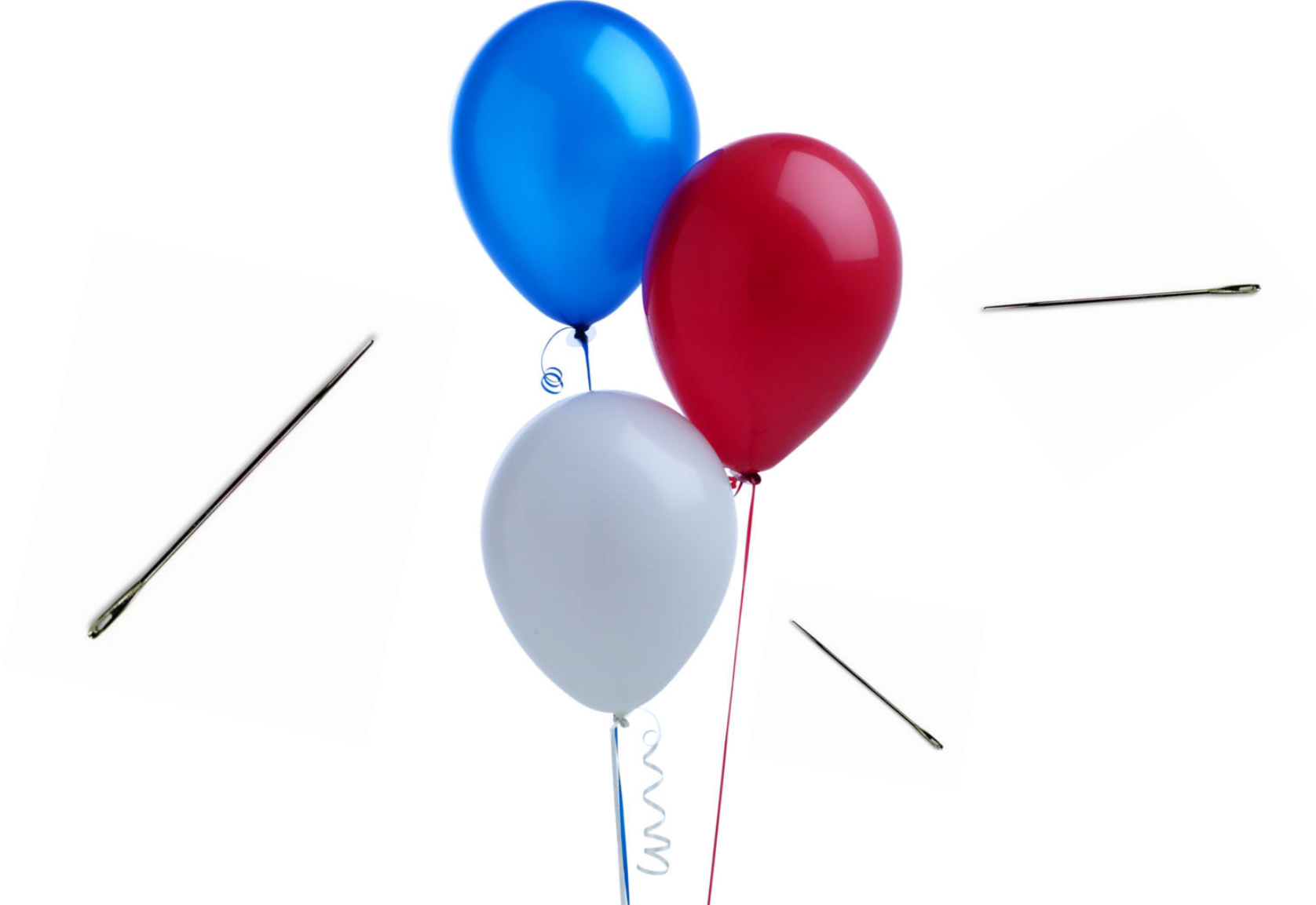
IDS systems that do not detect.

Staff do not seem to be sufficiently aware

Why Not?

Despite Each Having Spent Millions on All The “Best” Security Products, Software & Consultants

Because They Didn't Know What They Didn't Know



Three balloons are visible in the background: a blue one on the left, a red one in the center, and a white one at the bottom. They are slightly out of focus and appear to be floating against a light blue gradient background.

**Because a Hacker only needs to probe for a single
weak spot somewhere,
where to try and stick a needle in.**

**Where You Need to Be Aware 24x7 of EVERY New possible
Spot a Hacker Can possibly Stick A Needle ANYWHERE in
YOUR Organization ANYTIME.**

The Defenders Dilemma

**An Attacker only needs to find One Weakness
while the Defender needs to find Every One.**

Question to YOU

Did you study any Attacks?
And Checked how your Company would fare?

Most used attack vectors 2-15 years old
Attacks via client systems
Elevated privileges

Why don't we fix them?

Lack of Budget ~~Yes/~~**No**/~~Maybe~~

Lack of Solutions ~~Yes/~~**No**/~~Maybe~~

Lack of skilled People ~~Yes/~~**No**/~~Maybe~~

Lack of Focus ~~Yes/~~**No**/**Maybe**

Other Priorities **Yes**/~~No~~/~~Maybe~~

How to Avoid a Bear Attack



How NOT to Avoid a Bear Attack



Face down

Hands over neck

Lie on stomach

How to Avoid a Bear Attack

You don't have to run faster than the bear to get away. You just have to run faster than the guy next to you."

— Jim Butcher

Three balloons are positioned in the top-left corner of the slide: a blue one at the top, a red one in the middle, and a white one at the bottom. They are tied together with thin strings.

How to Outrun a Cyber (Bear) Attack

As long as you have a bit better security measures in place than the next one, hackers MAY move on to find an easier target and attack someone else.

UK Banking industry comes under fire for number of data breaches reported to ICO

UK Freedom of Information request to the ICO to obtain the figures, which showed a 183 per cent rise in reported Data Protection Act breach investigations in the financial services industry over the last two years. The vast majority of those occurred in 2014, with no less than 585 separate incidents (of the 791 total) being reported last year alone, which was over three times the amount of reports from the legal industry.

Today's report, however, casts some major concerns over the mistakes they're making with the information entrusted to them, whether that be citizens' personal details or highly confidential reports about the economic future of the country.

After the new EU data protection rules come into force, these numbers are likely to rise, and quite possibly by a considerable amount, with the ICO able to impose even bigger penalties.

ITProPortal, 3 June 2015

<http://www.itproportal.com/2015/06/03/banking-industry-comes-under-fire-for-number-of-data-breaches-reported-to-ico/#ixzz3c79ZKdUT>

Business Risk Intelligence



Cyber threat Awareness

- **Know Your Attack Surface**
- **Know In Time of Attacks That MAY Happen**
- **Pro-Actively Defend Your Attack Surface**
- **Create A Cyber Security Awareness Culture**



Lets see what we can learn from the past.....

Learn from what worked Before









We are always fighting a majority

One or two smart security techos against hundreds of thousands of them hackers. You can never hire enough smarts to defend, so, you got to be smarter and look for other ways.

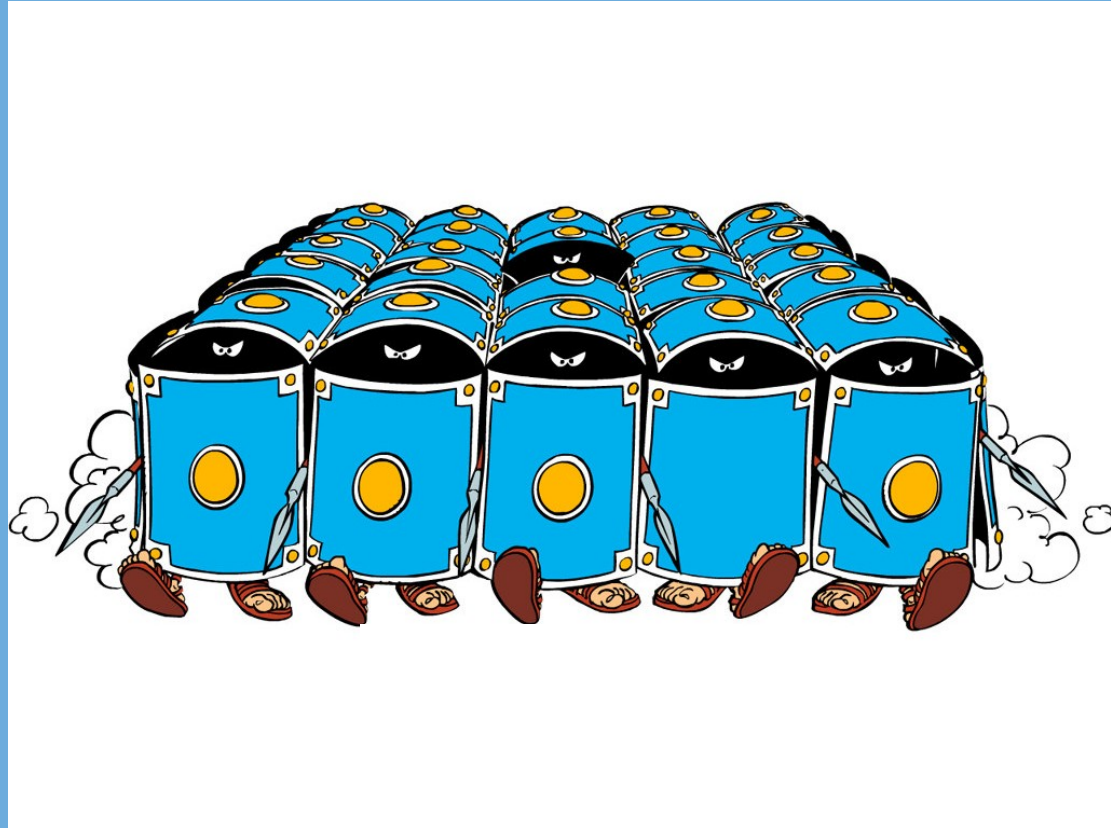
Follow traditional Roman Army Structure

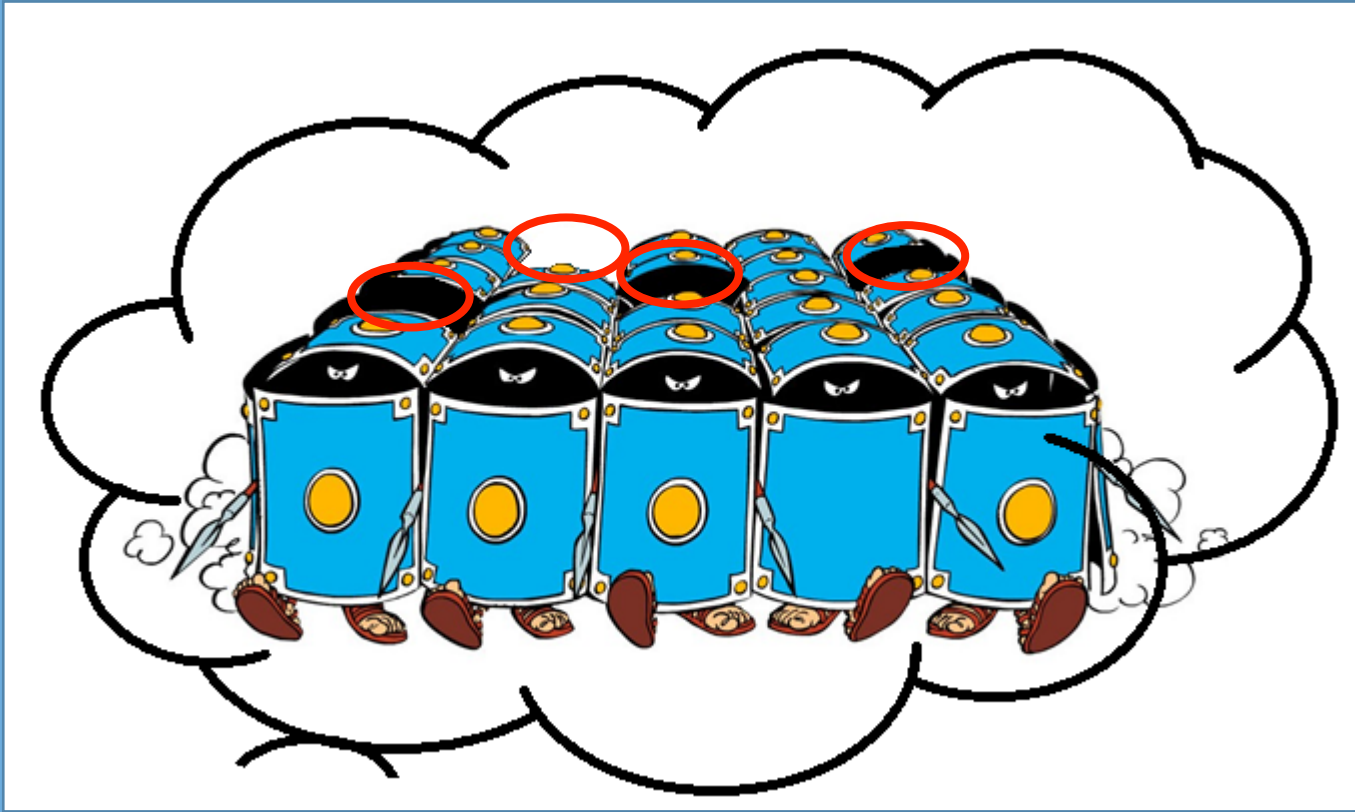
You need Footfolk and Knights on Horses

Each employee part of foot-folk

IT the Bow and Arrow Army

Security Experts the Horsemen





Every larger modern organization requires a multi-disciplinary Security Team. Cyber Specialists help IT managers determine where the digital dangers are lurking, can detect and trace a hacker attack, investigate it and do the forensics and minimize damage done while attacked.

HOWEVER, this type of beast is Scarce. Especially Incident Response Requires Unique Skills and Experience, you will have to look very hard to find them, and you have to pay them well.....

Business Users, Owners, Directors,
Business Management. C-Level,
Shareholders, Customers want to

PREVENT

IT-Security Experts
Love and Live to

FIGHT...

**IT-Security Professionals are NO ordinary IT people
Their modus Operandi differs considerably
from regular IT people.**

So, How do you keep these specialist motivated?

With great difficulty!!!!

The daily routine is boring!!!!



Cyberwarrior Shortage Threatens U.S. Security



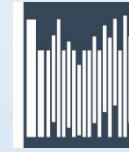
Experts Warn on Critical Shortage of Cybercrime Specialists



Senate Passes Cybersecurity Skills Shortage Bill



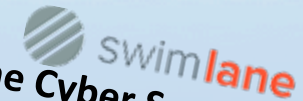
Government, Military Face Severe Shortage Of Cybersecurity Experts



Study: Shortage of security experts creating 'serious risk' for organizations



Shortage of Over A Million Cyber Security Experts Globally - Cisco



How the Cyber Security Talent Shortage Impacts Us All



Cybersecurity's hiring crisis: A troubling trajectory



Report: Shortage of cyber experts may hinder



Understaffed and at Risk: Today's IT Security Department



Big Data & The Security Skills Shortage



Surge in demand for senior cyber security experts as skills shortage hits



shortage of global specialists trained to confront increasingly malicious cyber security threats.



New research indicates cybersecurity skills shortage will be a big problem in 2015



'Blackmail' and 'fraud' used to recruit UK cyber experts



They are running WordPress.
Lets see what Plug-ins they've
got with it

X 1,834,556



Admin uses Adobe Acrobat
Reader. Load a juicy.exe
That will do the trick!!!

X 168,496



XSS All the Way,
XSS every day!!

X 345,665



X 219,887



A day not Hacked,
Is a day not lived..



X 749,217 X 420,376



Hit them with
that old office
exploit!!!

Why even bother
phishing if they leave
their backdoor wide
open?

Lets try a simple SQL
injection and then hit
them with that old
WordPress plug-in !!!



X 3,556,893



VANITAS
VANITATUM
OMNIA
VANITAS !

X 85,995

Whoopieeee, do I see a bunch
of JSPMyAdmin CSRF & XSS
Vulnerabilities on my path???





3 Small Problems:

1 There are not 10, but perhaps more than 10 million hacktivists, hackers, crackers, cyber crims, scriptkiddies and terrorists out there, And each one could potentially attack Your Organization and Cripple it

2 Your Newly Hired Boys Loooooovee fighting

3



There Aint No Silver Bullets.....

**OK, we set up an IT Security Department,
a CERT, or a CSIRT, as we call it..**

CERT – Computer Emergency RESPONSE Team

CSIRT – Computer Security Incident RESPONSE Team

RESPONSE







WHAT !!?
HACK AGAIN ?



*You mean you want to prevent those hackers from attacking us in the first place?? By fixing your locks ???????????
So you want to make it too hard for them, so they wont come in?????????????????*





YESSSSSSS!!!! Prevention may require discipline and be boring for you guys, but for the ORGANIZATION its A whole lot better to PREVENT.

A Whoooole Lot better.

Three balloons (blue, red, and white) are positioned in the top-left corner of the slide.

6 hard truths security pros must learn to live with

Never allow any undocumented network changes

Never allow any unmanaged open source software components

Always have IT patch, but always check the patch first on forehand

Thinking adding more security solutions will NOT solve the problem

You are doing your job RIGHT as long as nothing happens

Lack of understanding at Sr management level

Three balloons are positioned on the left side of the slide: a blue one at the top, a red one in the middle, and a white one at the bottom. They are tied together with strings.

One more hard truths security pros
must learn to live with

UNFORTUNATELY
THERE IS NO GLORY IN
PREVENTION

Three balloons are positioned in the top-left corner: a blue one at the top, a red one in the middle, and a white one at the bottom. They are tied together with strings and have small bows.

One more hard truths security pros
must learn to live with

DISCIPLINE

So What to Do?

- 1. Fix those Vulns!!!!**
- 2. Fix those Vulns!!!! (there are more)**
- 3. Fix those Vulns!!!! (Still some more)**
- 4. Fix those Vulns!!!! (Still some really old ones)**
- 4. Discipline your Staff as the Romans did**
- 5. Create Working Rewards for your Security Experts**
- 6. Create Full Risk Awareness, throughout the Whole Organization**
- 7. Create Full Risk Awareness amongst your Third Parties, Contractors, Customers**
- 8. Make sure you have Better Security and Protection than your Con-Colleagues**

4. Instill Security Discipline in your Staff as the Romans did in their armies



5. Create Working Rewards for your Security Experts

How to keep them happy? CSO formulated a list of recommendations :


- 1 – Step Back, Give them space**
- 2 – Give them the tools, but be realistic**
- 3 – Listen to ideas and value their knowledge**
- 4 – Provide fresh incentives**
- 5 – Encourage Competition**

Understanding what - really sought after – security experts motive is difficult. You have to know precisely what motivates each one of them, and whats important In their lives, inside, as well as outside of the office. In the longer term is Inspiration alone not enough. Financial rewards only motivate temporarily, In the First Financial Bank they work with rewards, and have found that training and competitions are important drivers to retain energy.

Looking at the bigger picture, most companies face the same universal security threats and challenges, so the biggest differentiators that an employer can offer, other than salary, are engagement and growth.

<http://www.csoonline.com/article/2926814/infosec-staffing/5-tips-for-keeping-your-incident-response-team-happy.html>

So, to be Able to -or at least Try to - Prevent, you HAVE to:

Three balloons are positioned on the left side of the slide: a blue one at the top, a red one in the middle, and a white one at the bottom. They are tied together with strings.

**Besides having deployed all the traditional
Security Software and Systems you also need to:**

Know Your Attack Surface

Know Ahead in Time Of Attacks That MAY Happen

Pro-actively Defend Your Attack Surface

Support A Security Awareness Culture

So, to be Able to -or at least Try to - Prevent, you HAVE to:

Like the Chinese Doctor Saying

As long as the Patient is Healthy, he will pay the doctor
The moment he gets sick, he stops paying

Always Remember,
Its in your Interest to Prevent

Not to Having to Mend



Business Risk Intelligence



Cyber threat Awareness

Questions?

Business Risk Intelligence and Alert Service

Fore-Warned is Fore-armed

[**https://brica.de**](https://brica.de)

Arjen de Landgraaf

Search Engines

- **Google type Search engines only cover max. 15% of total Internet content; only that what can be indexed.**
- **Google type Search Engines rank results on popularity**

For Quality Risk Intelligence we need to locate the hidden needles in haystacks; a single RELEVANT item in a single search result, hidden within some 64 million other, irrelevant items

Different Crops Require Different Harvesting Methods



Some need to be harvested by hand



Each single raw result need checking by one or more BRI Risk analysts



Pro-Active, Actionable Risk Intelligence



- Why investing in preparation up front is more valuable than investing after a breach occurs
- The key people, process and technology components of an effective incident management program
- The difference between the wise way and the risky way to manage an incident, through real examples
- How the evolution to proactive services will improve your security framework
- Rate your current tools' effectiveness versus advanced threats
- Recognize the difference between preventing attacks and detecting infections
- Take a forward-thinking approach to stopping data theft after compromise occurs
- Shift your Tier 2 & Tier 3 security teams from chasing alerts to solving long-term security challenges