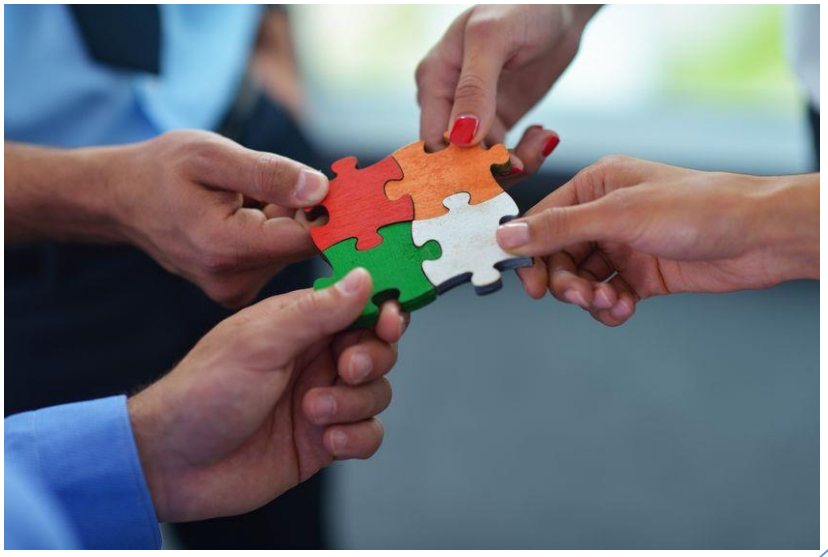
Business Profiles
Incorporated

The holistic approach

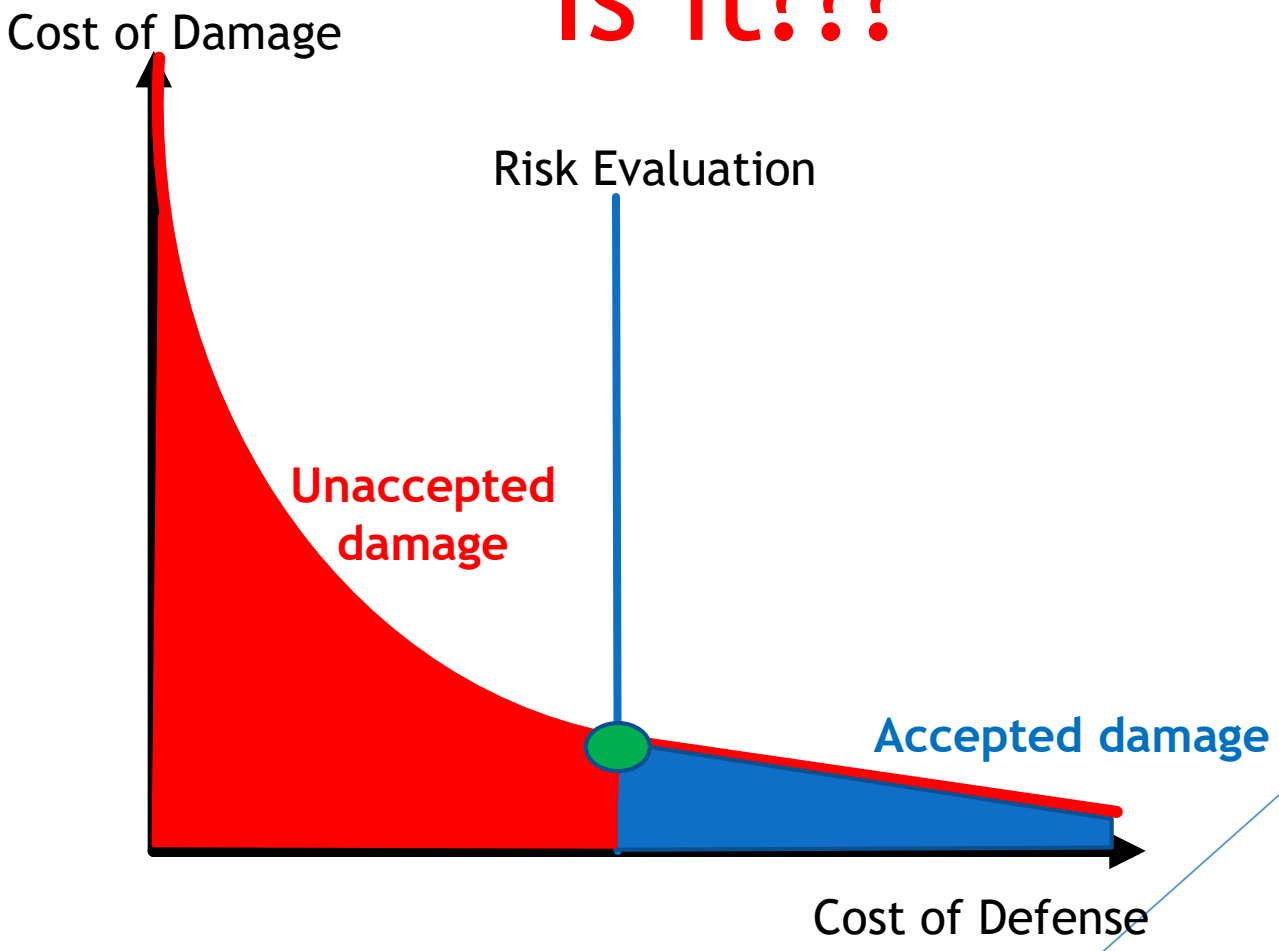
towards

A balanced and cost-effective cyber defense system



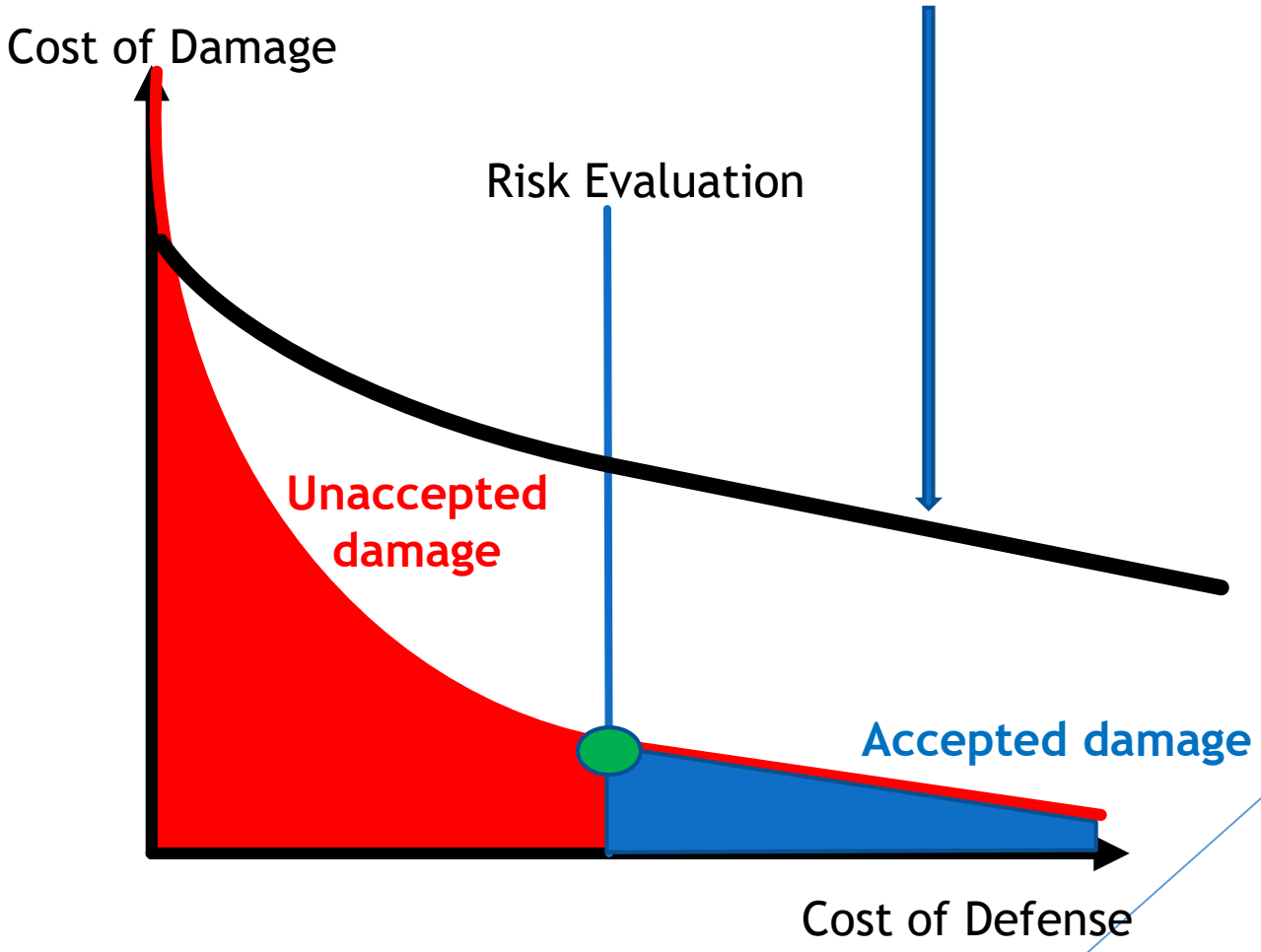
Risk analysis- The Whole Story

Is it???



Expect the Unexpected

The nonlinear development- The surprise



Business Profiles
Incorporated

So, How to build a **Cost Effective** Cyber Defense

Short analysis of Actors and factors

The Actors: Who are the Cyber Defenders?

- You and me and the last sale point operator- All of us?
- The IT team?
- The MSSP?
- The CICO?
- The SOC?
- The Technology we bought (So expensive…)?
- All the above?

The Eco System

Business Profiles Incorporated

- What are the boundaries of our Cyber domain?
  - ★
- What are our cyber assets?
  - Our docs. Our plans (commercial and private)?
    Our applications (online banking, personal…, company's tailor-made)
    Our passwords.
    Personal information (contacts, credit card, address, bank accounts).
    Third Party software
- Who wants to harm us? And Why?
  - Yes…. and Business intelligence specialists, Criminals, Our employees (?).
- Can we identify potential Threat/risk/problem
  - Yes… and No……..
- Can technology alone encounter threats?
  - Yes… and No……..

Why a holistic approach?

- undaries of our Cyber domain?
  - ps? And the Ipad? And the smartphone?
  - and private)?
  - ompany's tailor-made) Our
  - bank accounts)? Our
  - photos
- Where are these ass
  - Yes….. and all our portab
- Who wants to harm us? And Why?
  - Yes…. and Business intelligence specialists,
- Can we identify potential Threat/risk/problem
  - Yes… and No……..
- Can technology alone encounter threats?
  - Yes… and No……..

So,
Can we really do something about it ?
1st part of the password: Cyberprotection_

Decisions, Activities and….. Trends

- **Top managements do understand that:**
  - Significant and crustal asset of the entity are placed in the Cyber domain
  - The need to defend these assets requires special means….

1st part of the password: BPOCon

Decisions, Activities and….. Trends

Business Profiles Incorporated

- **Less understood are the following:**
  - The IT operation-teams can't focus on Cyber protection-
    It is not an added task. It is a profession.
  - Hacker are faster and better than the defenders.

It is an endless ongoing struggle

Decisions, Activities and….. Trends

- **Not well understood (if at all)**
  - Cyber attack's are not aiming toward IT assets….
    - **where is your money?**
      or
    - **How much are you willing to pay?**
  - **There is no "suddenly we were attacked…"**
    Cyber attack is a semi-military operation.
  - Data on attacks, Experiences and Crucial information **are not shared….**
  - **Crises-management while a Cyber event has only a little to do with IT**
    "right now" actions……
    (can you fix the problem?)

OMG…..So what to do?

Business Profiles Incorporated

- **IT manager's typical solutions**
  - Vulnerability assessments…
  - Lets buy more technology….
  - Lets outsource that task…
  - We need a tougher policy….

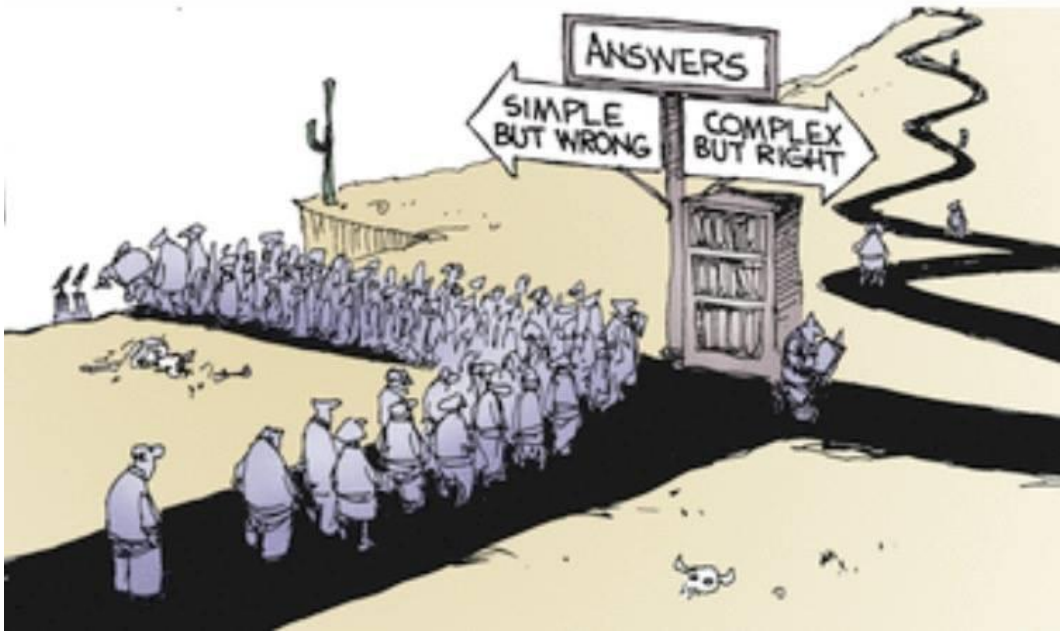
- **The CEO and board's typical questions:**
  - How much……. WOW…
  - And then, will we be protected???
  - Are we under attack already???
  - Can we do something else???

Corporate solutions include in many cases:

- **Additional tasks to the IT organization** with “We will do our best” approach.
- **Technology-tilt solutions** with less effective results than the expectations.
- **Late escalation of Cyber-problems**, if at all.
- **Outsource the Security-monitoring responsibility** without delegation of the business-continuity elements to encounter a cyber attack…..

The holistic approach

- How to build balanced Cyber defense capabilities?

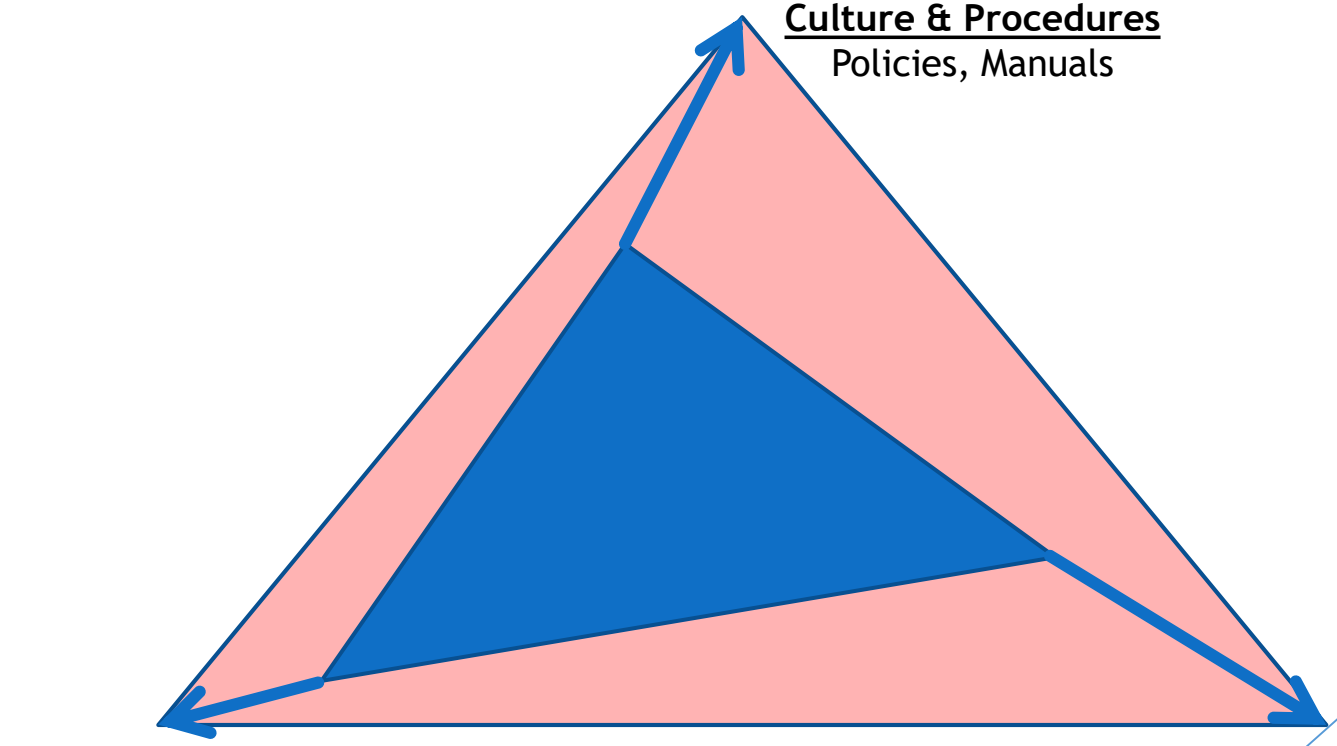


- What are the Dimensions of Cyber defense operation

Balanced Cyber defense capabilities

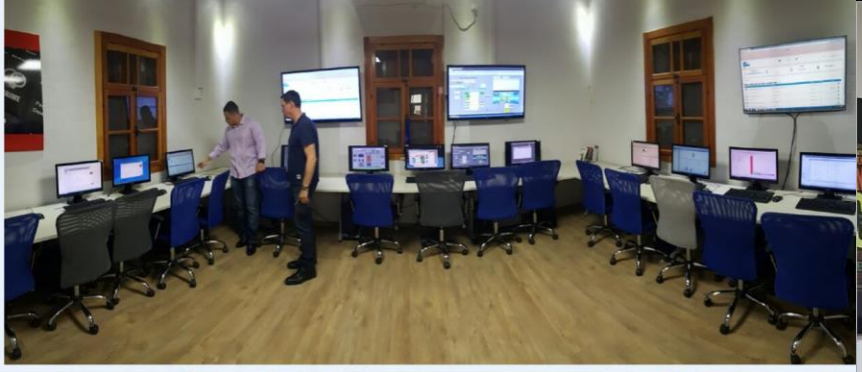
Tailor-made Balanced solutions

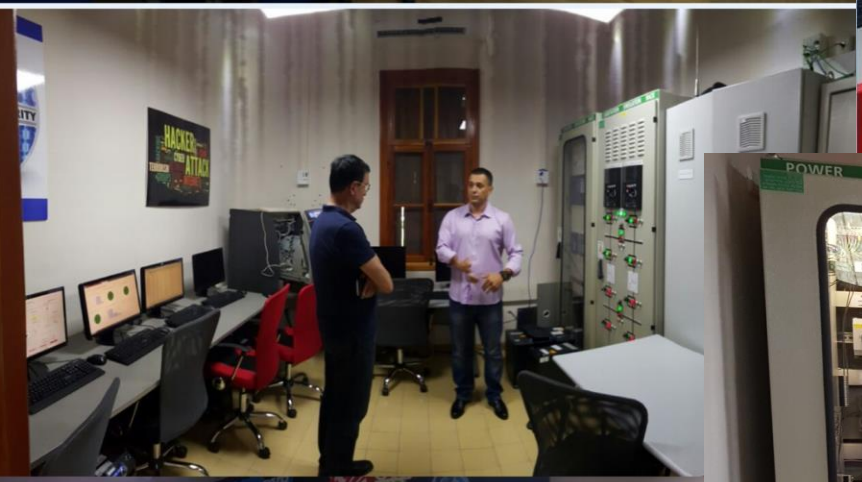
Cost effective implementation



Trainings – to whom and how?

- **Who is the targeted audience?**
  IT, SOC, CMC, Managements, Employees
  (Whom to train? firefighters or the residences?)
- **What to encounter?**
  The best updated threats
- **How to train against “Real” scenarios?**
  Our own configuration is a must!
- **Who can provide such trainings?**



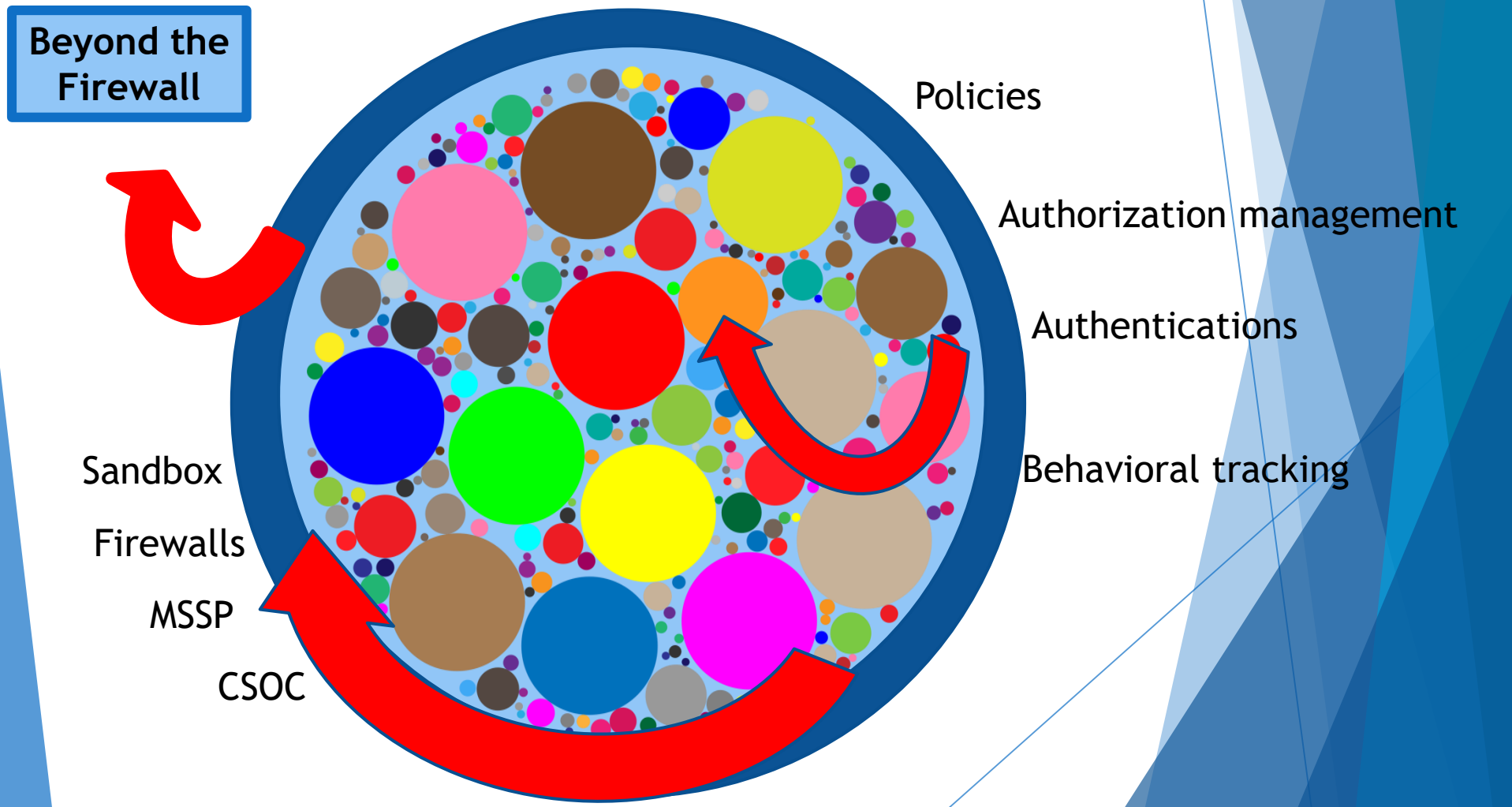

HACKER
ATTACK


VISA


Power Station Main Control Loops


POWER STATION PLC RACK-A
B.B. 380V
PLC-1
PLC-2
PLC-3
B.B. 24VDC
POWER STATION PLC RACK-B
B.B. 380V
PLC-4
PLC-6

Holistic Cyber defense operations



What is the meaning of Beyond the Firewall?

Can an organization get **threat-awareness capabilities?**

- **Yes, we can**
- **Should we?**
  - BI is there
  - Physical-threats intelligence is there
  - Market researches are there
  - OSINT is being used commercially (BI, profiling, etc)

- **And…..Webint is here!**
  - There is no “Sudden Cyber attack”
  - Alerting activities are in the darknet long before the attack is being launched.
  - Stolen credit cards, passwords, social connections, specific data-
    All can be bought over there
  - Webint commercial providers are available….
    A new profession is being developed

26-02-2017-001: Credit Cards Issued by mBank Selling on a Dedicated Marketplace in Past Fortnight

Threat Level

High

In the past weeks, we have identified details of 15 credit cards issued by **mBank** being sold on a dedicated marketplace. **We obtained partial, but indicative details** of these cards, **presented in an attached Excel file**, to aid in their identification and revocation. According to our assessment, the source of the breach could be a compromised payment systems of a company or business chain, in Poland or other country.

Threat Profile

Attack Vector	Threat Actor	Targeted Assets	Initial Recommendations
Data Leakage	Cybercriminals (Carders)	Customer Details	Cancel exposed credit cards if possible.

Sources	Relevance Sphere	Threat Credibility
Illicit Trading Platforms	Internal Asset or Specific Interest	High

Source Background: The data is offered for sale on dedicated marketplace, which are also advertised on closed carding forums. The credibility level of this marketplace is high, and the information it trades in assessed to be valid and authentic.

Threat Details

Our monitoring of online underground credit card data-trading platforms revealed a credit cards issued by **mBank** for sale on a dedicated marketplace. **According to our analysis, this marketplace currently holds the records of 15 mBank-related credit cards**. We were only able to obtain partial details of the cards, as it is impossible to obtain the entire data base without purchasing it. However, the partial data is sufficiently indicative and contains the full name of the card owner, the first seven digits of the card number, and its expiration date.

The dates that appear alongside the cards likely indicate the date when the data was uploaded to the marketplace, suggesting that the majority of the cards were stolen over the course of the past two weeks (February 14 – 25, 2017). The cards were traded on a shop that has offered huge numbers of stolen card details in recent months. We assume that the threat actors behind this shop have access to large databases originating in hacked e-commerce websites (they either hack them themselves or purchase the data from numerous hackers).

The price of each card is $12. Notably, the price is usually determined by the expiration and breach dates. Details of recently stolen credit cards that will not expire for a long time are sold for higher prices.

Cyber Threat Intelligence Alert

02-03-2017-001: Access to Banca Transilvania Database for Sale on a Russian Underground Forum

Threat Level

Severe

We noticed an offer to sell a root access to a database of *Banca Transilvania*, published on a closed Russian forum dedicated to cybercrime. The seller also uploaded the database dump as proof. Our analysis indicates with high probability that the data is authentic.

Attached is the full DB dump, in a text file.

Threat Profile

Attack Vector	Threat Actor	Targeted Assets	Initial Recommendations
Unknown	Cybercriminal	Database	• Verify the authenticity of the data. If the data is authentic and belongs to the bank, try identifying the leakage source. • Assuming that the root access was already sold to potential attackers, take measures to secure the data and minimize the attack damage.

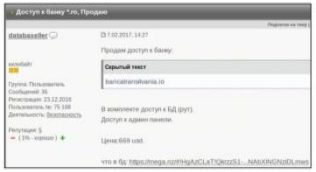
Sources	Relevance Sphere	Threat Credibility
Russian-language underground forum	Internal Asset or Specific Interest	Medium

Threat Details

On February 7, 2017, a member of a Russian password-protected forum posted a message offering to sell **a root access to a database of *Banca Transilvania***. According to the post, **access to the administration panel of the database is also provided**, meaning that the buyer will be able to modify the DB.

The price for the root access and the admin panel access is $669.

Figure 1: The initial sales thread



February 22, 2017

Cyber Threat Intelligence

Spora Ransomware: TECHINT Analysis

It wasn't raining when Noah built the ark

Howard Ruff

Please be aware that this document may contain links and attachments that if activated may lead to malicious websites or allow a malicious actor to collect information about the user.

Monthly Report
Cyber Threat Intelligence
for
A French Bank

It wasn't raining when Noah built the ark

Howard Ruff

Please be aware that this document may contain links and attachments that if activated may lead to malicious websites or allow a malicious actor to collect information about the user.

Bitcoin Extorting using DDoS attack on Greek banks – introduction

Background

Following the attack on 3 major banks in Greek you will find here our reports regarding the attack together with our recommendation

Previous Attacks & Intelligence Report

In the last few months we have been following this method of attack and we believe the group called **Armada Collective** conducting this attack while they adopted this method from another group called DD4BC.

On November 15th we have reported to our customers on expected attack together describing the method of the attack with our recommendation (see marked green in page 5 and 16 in **Annex A**).

We also advised our customer 5 month ago on the **FBI** Notification regarding ***"Bitcoin Extortion Campaigns expanding Distrusted denial of Service Attacks to wider array of Business Sector"*** **(Annex B).**

General Recommendations

- ***Phase 1***
  - Define and practice protocols for dealing with extortion. **We recommend you to refuse paying the ransom**.
  - Short and Immediate Testing the readiness of your security against DDoS attacks.
  - Contact your internet provider, so it can assist you in case of an attack:

1. BANKX FINANCIAL SPECIFIC INTELLIGENCE

1.1. Several computers within BankX Financial networks have been found infected with malware – immediate remediation required

RISK:	**High** (Four different malware families that may lead to the theft of credentials or other information)		
THREAT AGENT:	Cyber-criminals, Crime organizations	**PROVIDER AND SYSTEMS AFFECTED:**	Personal computers, servers
RELEVANCE:	BankX cyber security	**TARGET AUDIENCE:**	Cyber and IT
CREDIBILITY:	High		
SOURCES:	Sinkhole – monitoring command and control bot servers		
RESULTS:	Computers within BankX's networks 999.29.92.0/22 and 998.92.0.0/16 are infected with four malware types, and have been communicating with C2 (command and control) servers. Potentially, sensitive information has been leaked for fraud or other crime activities. Criminals might still have access into the network.		
RECOMMENDATIONS:	• Investigate communication and DNS logs in order to find the computers that have been communicating with the command and control servers. • Upon locating infected computers, perform incident response activities. Remediation tools, specific investigation, and forensic methods exist for the mentioned malware. We would be happy to provide them upon request.		

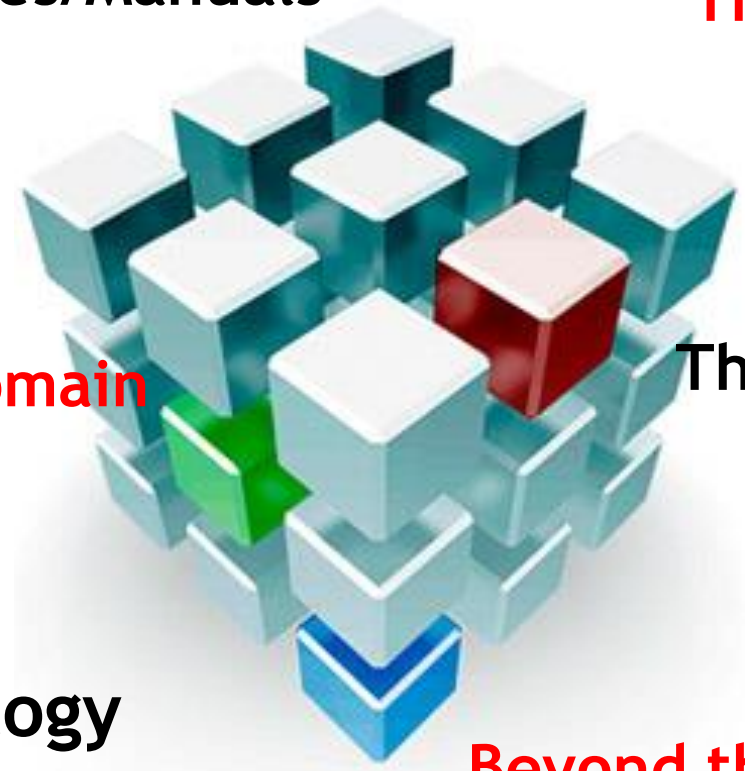
When computers are infected with different types of malware, they become a part of a network (botnet) of infected computers (bots). Bots send information they collect from the infected computer and perform other malicious activities. The information is sent to a command and control server, which might send back commands to the bot. There are various methods to intercept/capture this communication, in order to learn about infected computers in the botnet.

Using sinkholing techniques, we were able to intercept IP addresses within BankX's 199.29.92.0/22 and 197.92.0.0/16 networks, communicating with the C2 servers. The latest communication we have detected is between APT Sykipot malware and its C2 server, on October 2015. Also, we found a number of previous infections from 2013-2014. We have found a Sality bot infection communicating

The Holistic approach to encounter Cyber threats

Culture/Policies/Manuals

The cyber boundaries



The inner domain

The Human-Resource

Technology

Beyond the Firewall

Business Profiles
Incorporated

Thank you

As for the password-

Joke lang ☺