
# Segurança da Informação: Não jogue com os dados

## SECOVI-SP

**Domingo Montanaro -** 15/03/2022

# Cybercrime

The IoT is also amplifying the potential cyberattack surface. It is estimated that there are already over 21 billion IoT devices worldwide,[15] and their number will double by 2025.[16] Attacks on IoT devices increased by more than 300% in the first half of 2019,[17] while in September 2019, IoTs were used to take down Wikipedia through classic distributed denial of service (DDoS) attacks,[18] and the risk of IoT devices being used as intermediaries is expected to increase.[19] In 2021, cybercrime damages might reach US$6 trillion[20]— what would be equivalent to the GDP of the world's third largest economy.[21]

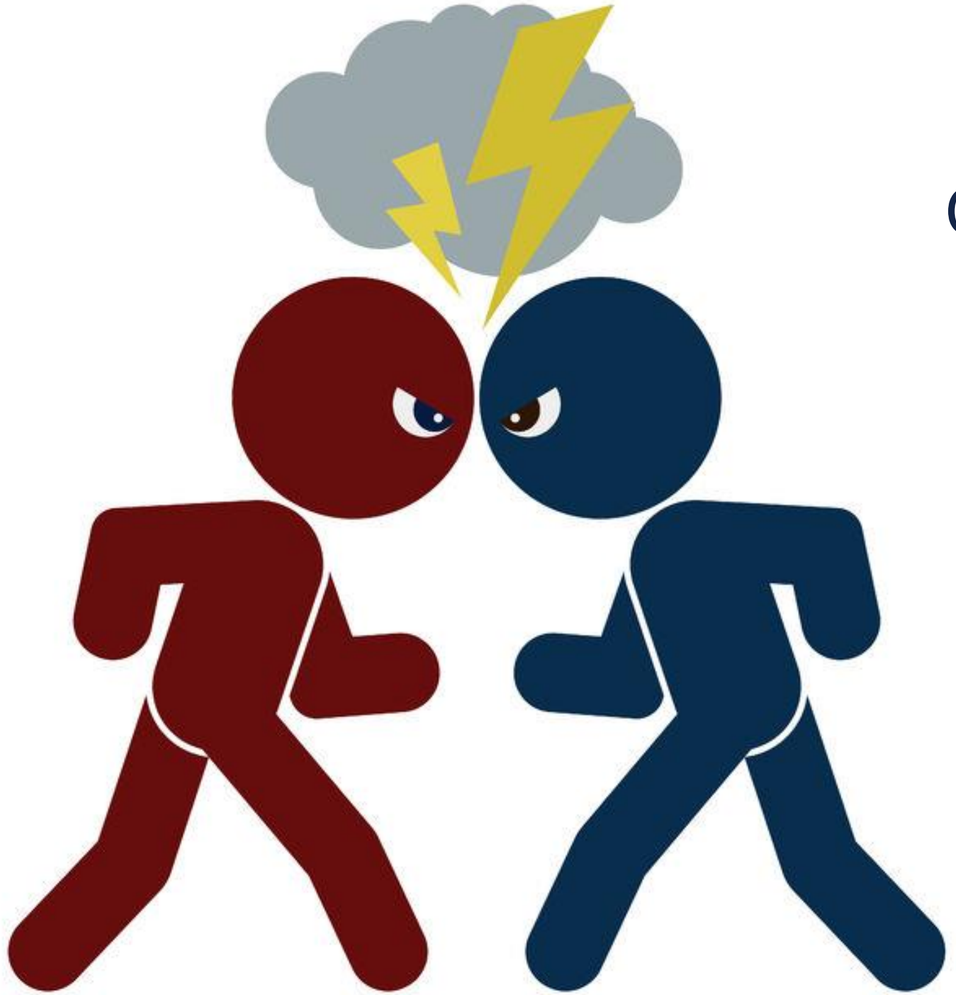
# Cybercrime

- ‘Pure cybercrime’ refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.

- Traditional forms of crime have also evolved as criminal organizations turn increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. These ‘cyber-enabled’ crimes are not necessarily new – such as theft, fraud, illegal gambling, the sale of fake medicines – but they have taken on a new online dimension.

Definição da Interpol (https://www.interpol.int/Crimes/Cybercrime)

# Quem pratica um cyber attack?



O adversário!

# Quem sobrepuja as barreiras de segurança?

Top stories

Hackers invadem sistema de casa e infernizam moradores

Olhar Digital · 2 days ago

Vândalo

Hackers norte-coreanos invadem caixas na Índia

Olhar Digital · 2 days ago

Ladrões

Governo quer deixar país menos exposto a hackers

Olhar Digital · 19 hours ago

Espiões

→ More for hackers invadem

Hackers invadem sistemas da NSA e liberam material na ...

https://tecnoblog.net › Antivírus e Segurança ▾ Translate this page

O grupo de **hackers** The Shadow Brokers afirmou nesta terça-feira (16) que foi responsável por uma invasão nos sistemas da NSA, a agência de inteligência ...

Ativistas


THE
MARTIAN
ARE COMING
TO SAVE
THE EARTH

# Hackers notáveis (90s and 2000s)




# Hackers em 2009

JP Edição 23,021 - Índice Geral
Ano 58 – Terça-feira, 07 de julho de 2009

Polícia

**Publicado em:** 07/07/2009



## Quadrilha de hackers é presa tentando roubar BB de Santa Inês

# Em menos de 13 anos…

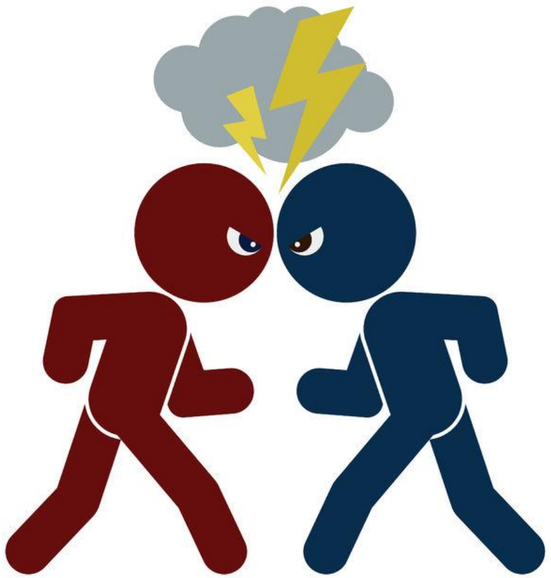

**“Hacker” in 2009**

## ➔Threat Transition

- Mesma motivação?
- Mesmo contexto?

# Seguro… contra quem?

Quem é o adversário / threat actor do seu negócio?



| Threat Actor | Motivação |
|---|---|
| Gangue especializada | Financeira |
| Gangue amadora | Financeira |
| Ex-funcionário | Passional |
| Funcionário | Ideológica / Financeira / Passional / Concorrencial |
| Concorrente | Comercial |
| Exércitos (Estados) | Espionagem/PI |
| Ativista | Ideológica |
| Receitas (Estado) | Fiscalização |
| Polícias (Estado) | Investigação de delitos |
| Sócio | Concorrencial |
| Acionistas | Fiscalização |
| Script Kiddie | Curiosidade / Ego |
| Worms / Robôs | Coleção de ativos |
| Fornecedor | Financeira |
| Sindicato | Política |
| Órgão regulador | Fiscalização |
| Imprensa | Tração / Clientela |

# Quando o papo é segurança e quando o papo é privacidade

Cyber Risk Education

i. Quem são os adversários?
ii. Quais são suas motivações?
iii. Quais são as jóias da coroa do meu negócio?
iv. Quais são as ameaças?
v. O que eu vou fazer a respeito?

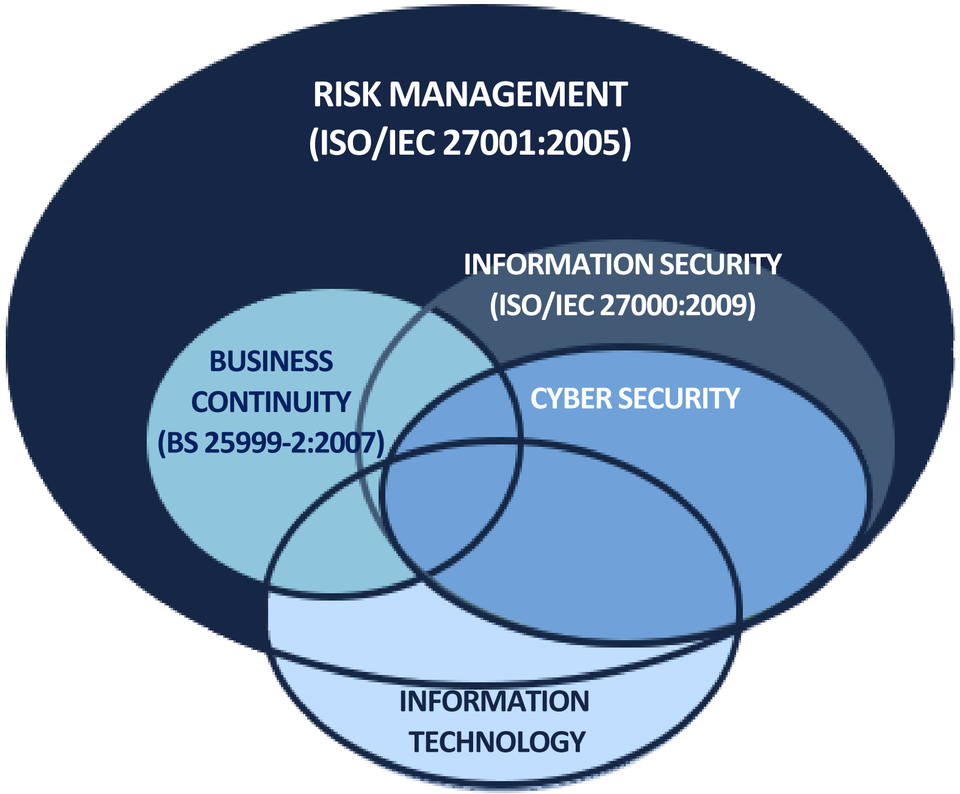
‘Cyber risk’ means any risk of financial loss, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems. (IRM)


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Focos das áreas de Ti e cyber security de pequenas e medias organizações

Papo anos 90 (cheque = bala de prata):

- “Precisamos investir em segurança”
- “Ok, qual anti-virus a gente compra?”



# Visão macro : nível estratégico

0. Cyber Security é um **business problem** e não um technical problem.

1. **Jóias da coroa**: quais são?

2. Unidades de negócio têm que prover recursos ($ e **tempo**) para mitigar cyber risk.

3. Sessões privativas com responsável por cyber (que tenha envergadura corporativa)

    --> O que te preocupa?

    --> Como eu posso ajudar?

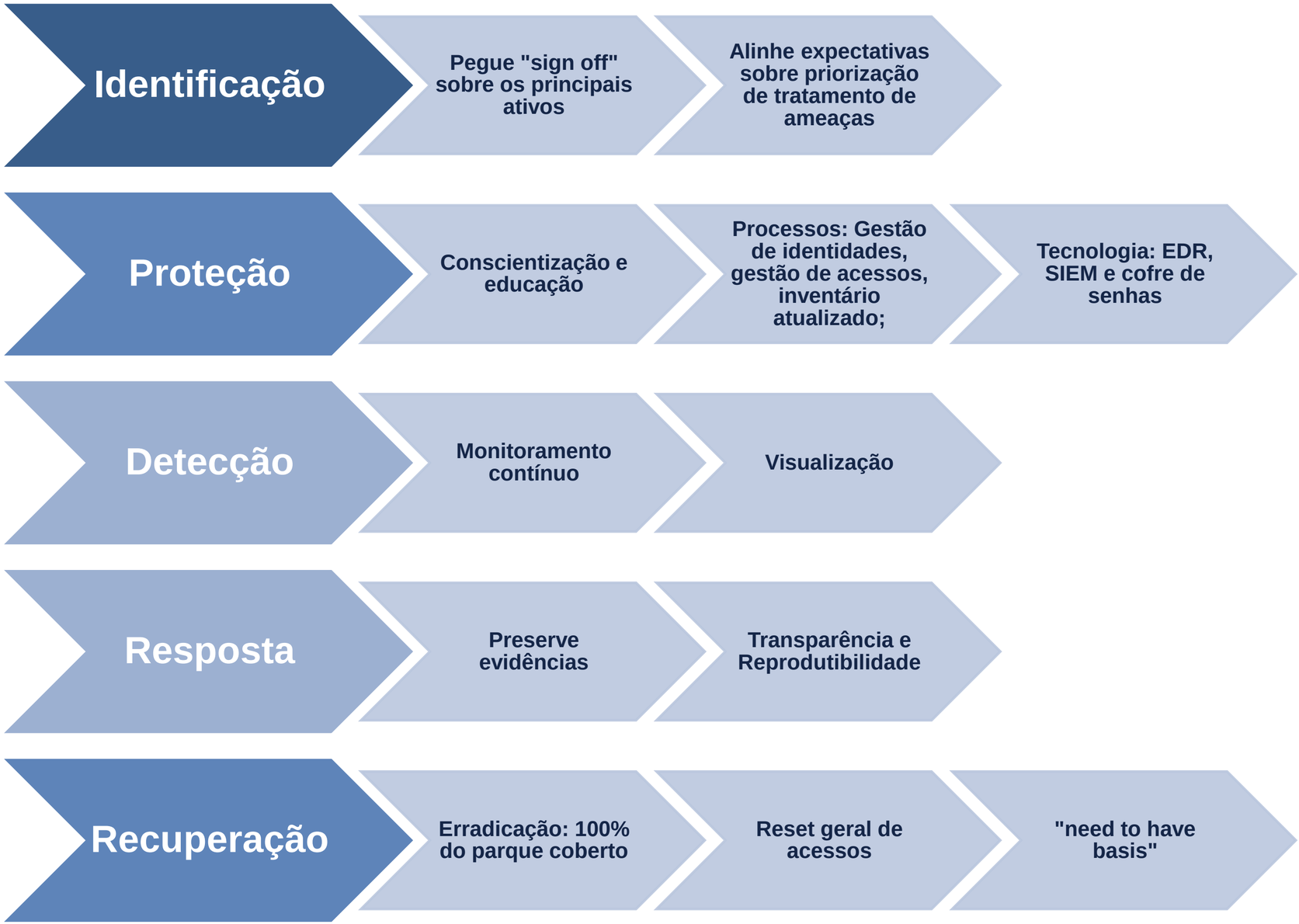
4. **Educação e conscientização** --> O que você está fazendo a respeito?

5. Troque experiências com outras organizações e aprenda com os erros deles. Não espere ser vítima de um incidente para ter suas proprias “lições aprendidas”

6. Você está preparado para um incidente, sob a ótica de tudo que não engloba proteção?

Ex: Trilha de auditoria, contratos com fornecedores, seguros, etc.?

# Visão Micro: Cyber Security Framework: “o básico”



MAY 11, 2021

# Cyberattack halts fuel movement on Colonial petroleum pipeline

**Petroleum product supply overview**
U.S. Gulf Coast and East Coast regions

# Causa raiz?

Cyber Risk Education

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a **single compromised password**, according to a cybersecurity consultant who responded to the attack.

Hackers gained entry into the networks of Colonial Pipeline Co. on April 29 through a virtual private network account, which allowed employees to remotely access the company's computer network, said Charles Carmakal, senior vice president at cybersecurity firm Mandiant, part of FireEye Inc., in an interview.

**https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password**

ESTAMOS À DISPOSIÇÃO!

# OBRIGADO!

**Domingo Montanaro**
**domingo@venturaerm.com**

**ACESSE AGORA:**
**WWW.VENTURA.AC**

Capacitação para leigos e especialistas