



# Varená žaba a odolnosť voči rizikám v kybernetickej bezpečnosti

EFOCUS: RIZIKÁ A ICH MANAŽMENT V KYBERNETICKOM PRIESTORE A V PODNIKOVEJ IT INFRAŠTRUKTÚRE



**Ivan Makatura**  
IBM Slovensko, s.r.o.

# Syndróm varenej žaby...

- Nechá sa žaba dobrovoľne uvariť...?
- Nie. Vyskočí z vody, ihneď, ako zistí, že je voda príliš horúca.
- Reakcia podnikov na riziká v oblasti kybernetickej bezpečnosti je podobná:
  - Uvedomujete si, že riziko stúpa – chcete sa chrániť pred útokmi.
  - Ako vyskočiť z nepríjemne horúcej vody...?
- Obmedzenia:
  - Štatistika a „papierové“ opatrenia riziká reálne nevyriešia
  - Kvalifikovaných bezpečnostných profesionálov je nedostatok
  - Náklady na bezpečnostné opatrenia nemôžu stúpať donekonečna
  - Nepremyslená a nenaplánovaná implementácia technických opatrení nemá účinnosť
- Jestvuje však cesta von z „horúcej vody“:
  - Kybernetická odolnosť („Cyber Resiliency“) je program, ktorý môže zaručiť schopnosť organizácie pokračovať v štandardných procesoch aj po incidente, iba s minimálnym prerušením
  - Kybernetická odolnosť je širším pojmom, ktorý zahŕňa riadenie rizík, informačnú a kybernetickú bezpečnosť a riadenie kontinuity činností.



# World Economic Forum: The Global Risks Report 2018

## Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Natural disasters
- 3 Cyberattacks
- 4 Data fraud or theft
- 5 Failure of climate-change mitigation and adaptation
- 6 Large-scale involuntary migration
- 7 Man-made environmental disasters
- 8 Terrorist attacks
- 9 Illicit trade
- 10 Asset bubbles in a major economy



## Top 10 risks in terms of Impact

- 1 Weapons of mass destruction
- 2 Extreme weather events
- 3 Natural disasters
- 4 Failure of climate-change mitigation and adaptation
- 5 Water crises
- 6 Cyberattacks
- 7 Food crises
- 8 Biodiversity loss and ecosystem collapse
- 9 Large-scale involuntary migration
- 10 Spread of infectious diseases

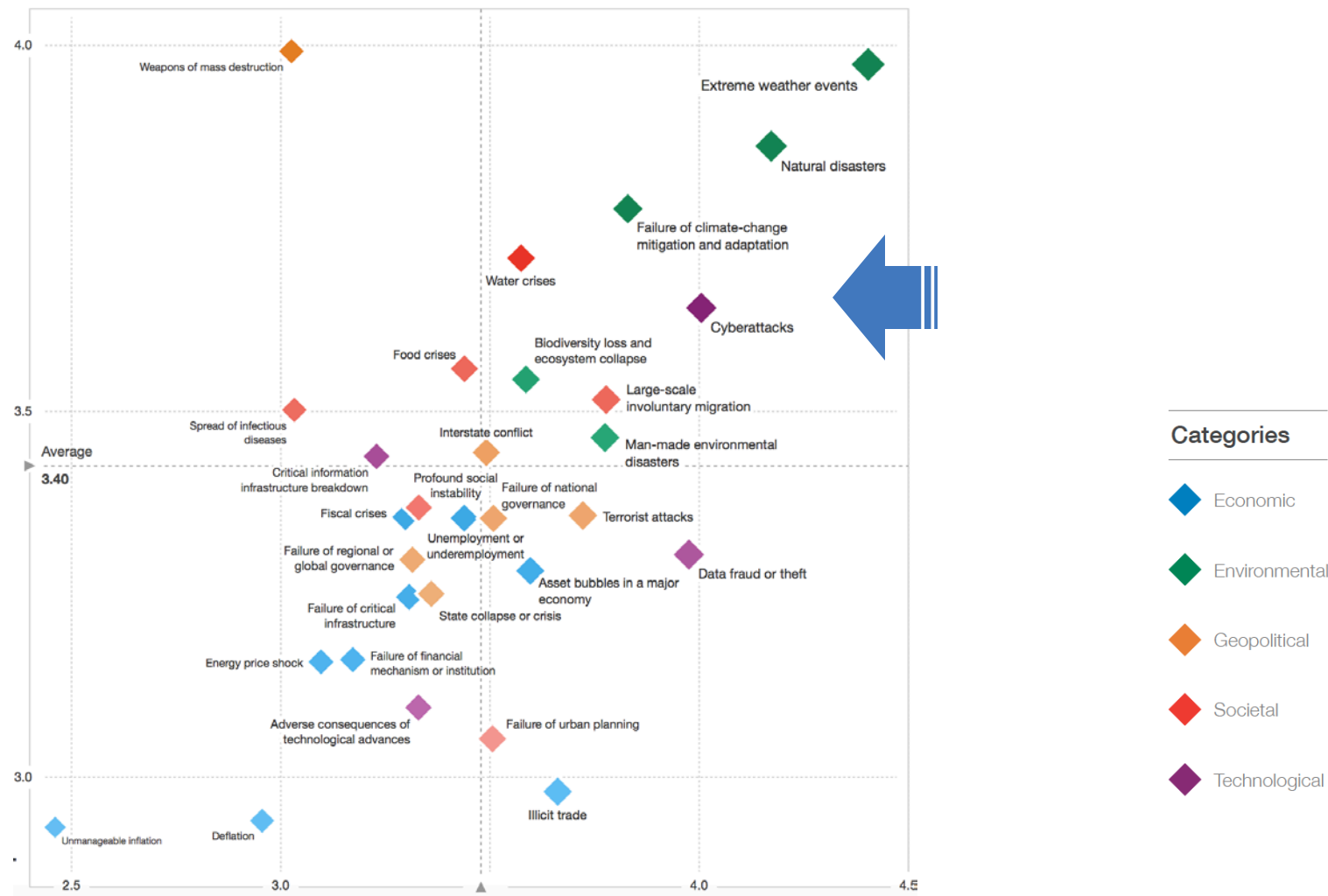


## Categories

- Economic
- Environmental
- Geopolitical
- Societal
- Technological

[http://www3.weforum.org/docs/WEF\\_GRR18\\_Report.pdf](http://www3.weforum.org/docs/WEF_GRR18_Report.pdf)

# World Economic Forum: The Global Risks Report 2018



# Rýchle zotavenie sietí a informačných systémov po kybernetickom útoku je pre organizácie náročnou úlohou...



**01**

- Obnova činností trvá z hľadiska biznisu prídlho
- Testovanie plánov obnovy má dopad na bežnú prevádzku



**02**

- Dynamicky sa rozvíjajúce IT prostredia znižujú efektivitu BCM



**03**

- Regulácia prichádza z novými (mnohokrát nezmyselnými) požiadavkami

# Cieľom útoku sú typicky aj záložné riešenia



- 01** • Útok často spôsobí kompromitáciu aj záložných riešení
- WannaCry / WannaCrypt0r / CryptoLocker



- 02** • Na obnovu činností má organizácia limitovaný čas, zatiaľ čo útočníci majú priestor na opakovaný útok aj obnovených riešení



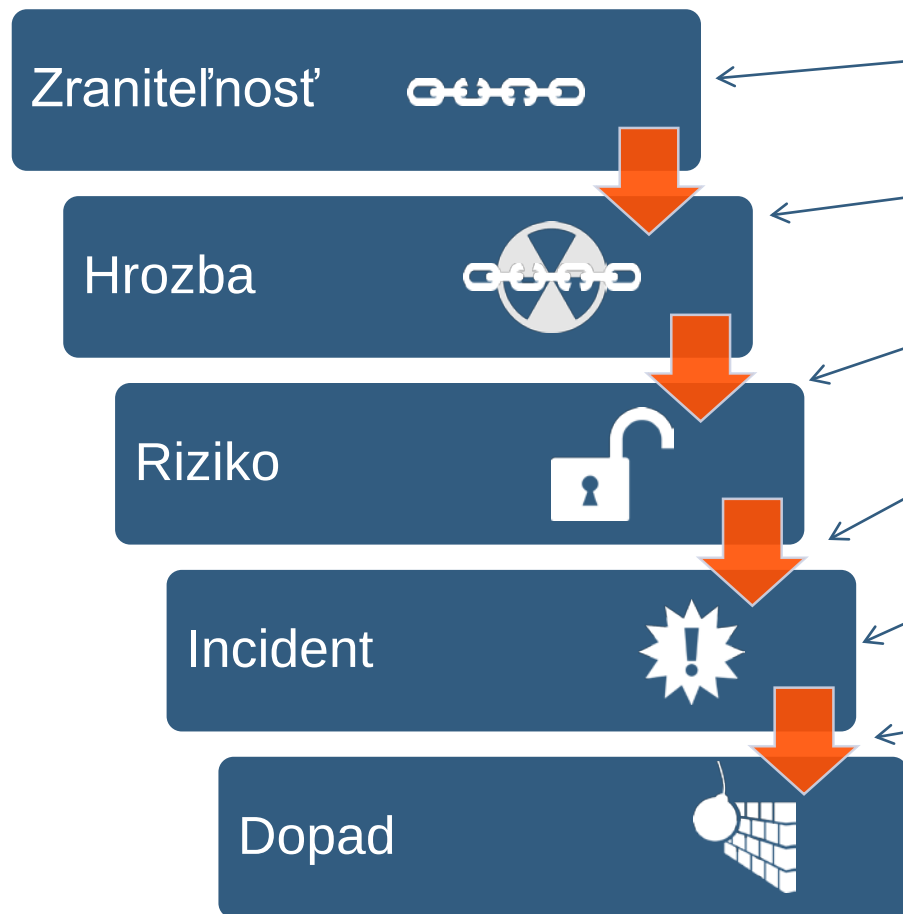
- 03** • Cieľový čas obnovy (RTO) a cieľový bod obnovy (RPO) sú pre dnešné potreby už nedostatočné



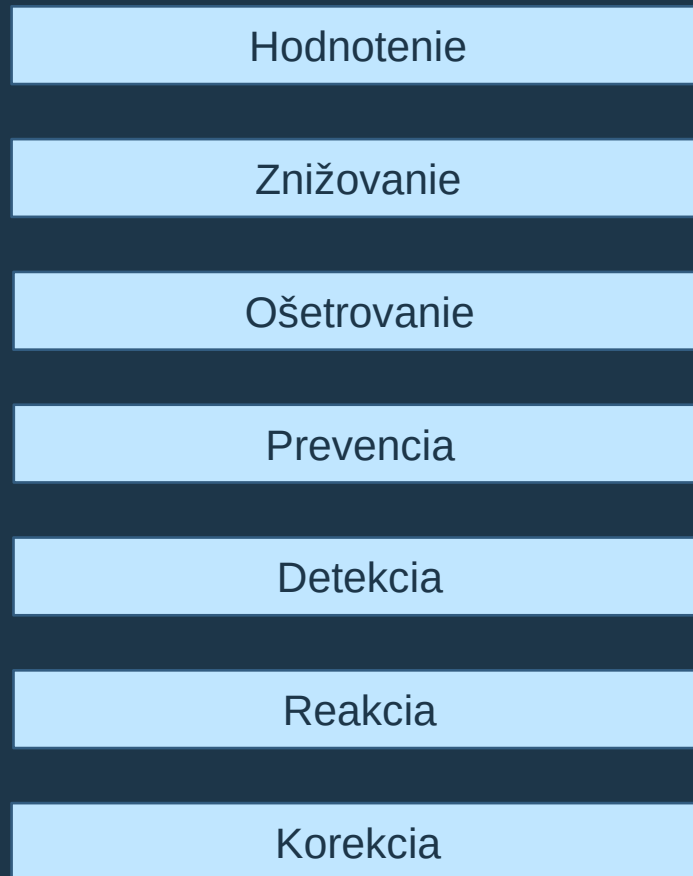
# Kybernetická odolnosť



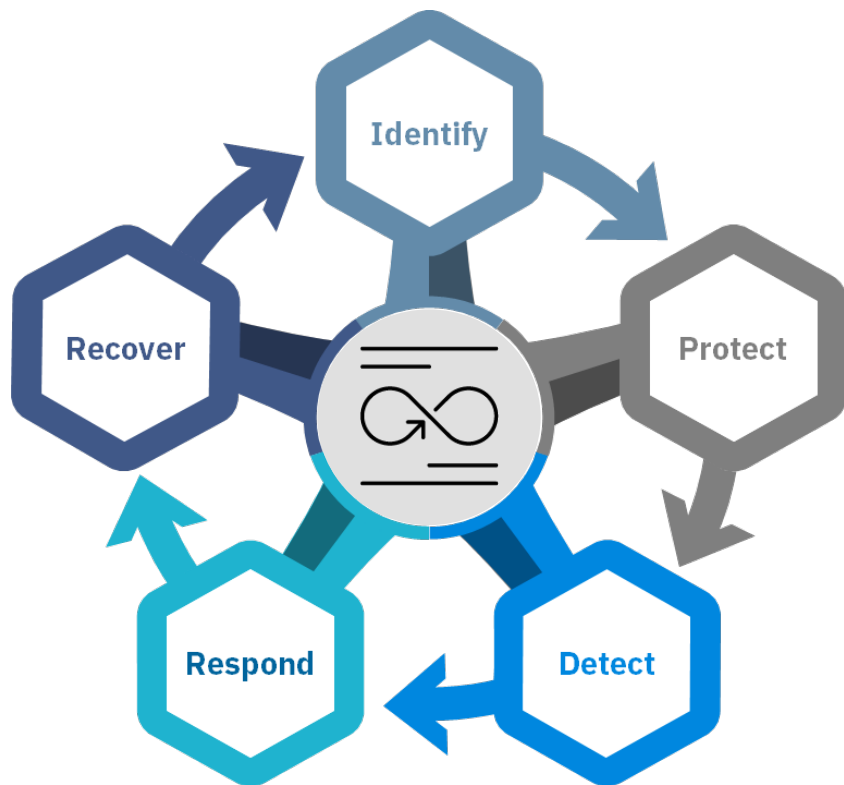
# Životný cyklus incidentu



## Kategórie opatrení:



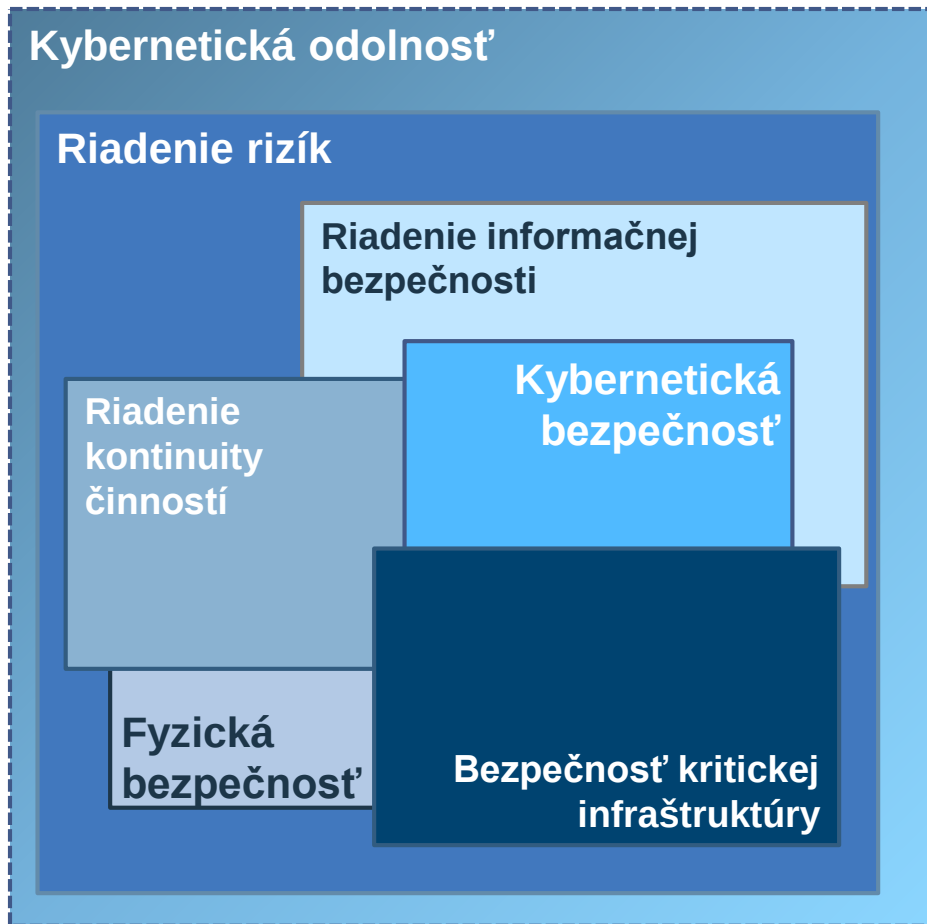
# Rámec "Cyber Resiliency"



- **Identify** (Identifikovať) počiatočný krok v dosiahnutí kybernetickej odolnosti
- **Protect** (Chrániť) proti útokom identifikáciou a hodnotením zraniteľností skôr, než sú zneužitú hrozbou
- **Detect** (Detegovať) neznáme hrozby pokročilou analytikou
- **Respond** (Reagovať) efektívnym riešením v priestore kritických aktív
- **Recover** (Obnoviť) zo škôd spôsobených útokom

\* Životný cyklus "Cyber resilience" je založený na technickej norme NIST Cybersecurity framework.

# Odolnosť voči hrozbám je kombináciou viacerých disciplín



|                      |                               |
|----------------------|-------------------------------|
| Organizácia          | Technologické prostredie      |
| Ochrana údajov       | Klasifikácia informácií       |
| Riadenie IT rizík    | Manažment zraniteľností       |
| Havarijné plánovanie | Security Governance           |
| IT architektúra      | Riadenie aktív                |
| Riadenie prístupov   | Riadenie zmien a konfigurácií |
| Riešenie incidentov  | Service Level Management      |
| Vzťahy a komunikácia | Biznis architektúra           |
| Ekosystém partnerov  | Vzdelávanie a povedomie       |



# Kybernetická odolnosť

- **Kybernetická odolnosť** je schopnosť organizácie kontinuálne pokračovať v činnosti s najmenšou mierou narušenia počas kybernetického útoku

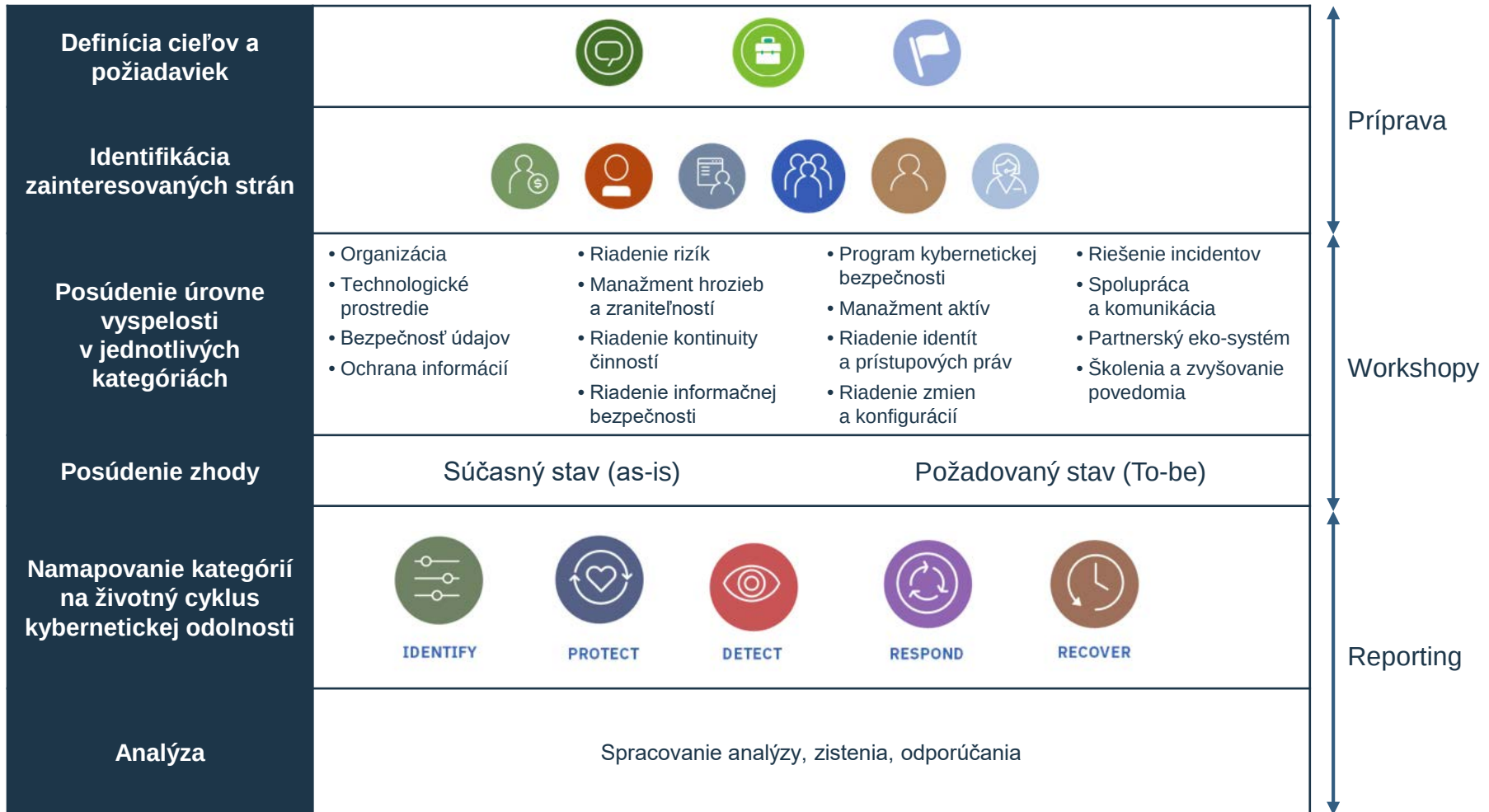


- **Cyber Resilience** je iniciatívou, ktorá spája a rieši niekoľko kritických oblastí:
  - informačnú bezpečnosť,
  - riadenie IT služieb
  - kybernetickú bezpečnosť a
  - riadenie kontinuity činností

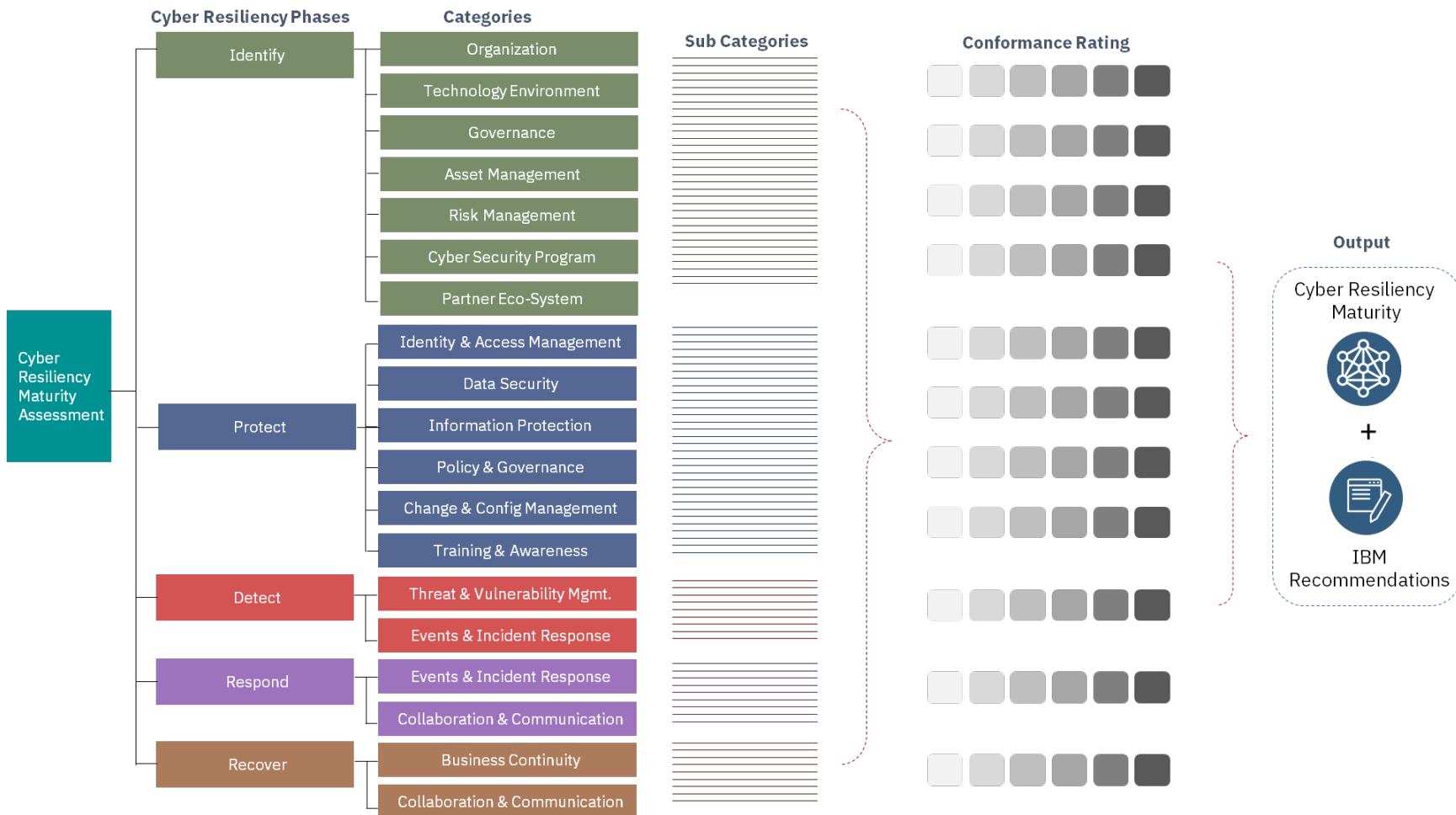
aby produkty a služby boli aj v prípade ich prerušenia dodávané na vopred definovaných úrovniach, s cieľom vyhnúť sa poškodeniu dobrej povesti a obchodnej značky

- **Kybernetická bezpečnosť** je stav, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov
- **Riadenie kontinuity činností** je holistický podnikový riadiaci proces, používaný na ochranu záujmov zainteresovaných strán, reputácie, obchodnej značky a činností vytvárajúcich hodnotu zabezpečením pokračovania prevádzky aj v prípade incidentu.

# Prístup k posúdeniu úrovne kybernetickej odolnosti



# IBM rámec posúdenia kybernetickej odolnosti

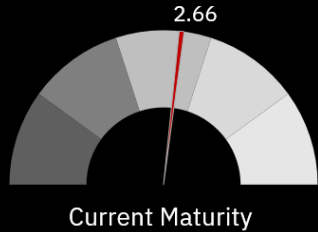




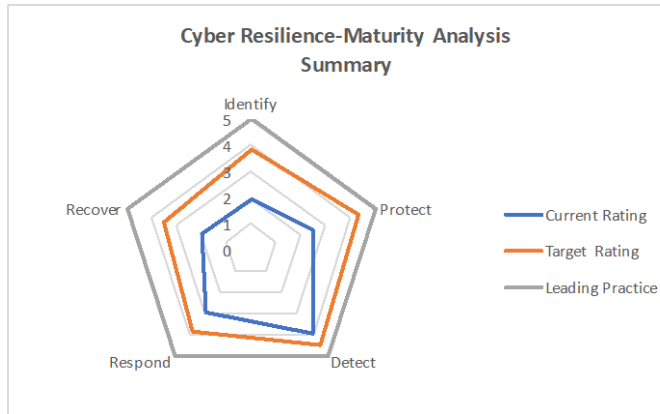
# Príklad Cyber resilience report-u



# Management Summary



## Summary



## Current State

- <client> has fairly matured IT processes. However lacks a formal cyber resiliency charter. While the current Security processes and systems are well poised to handle traditional threats and vulnerabilities, it is not completely geared up to meet challenges posed by cyber threats.

## Areas for Improvement

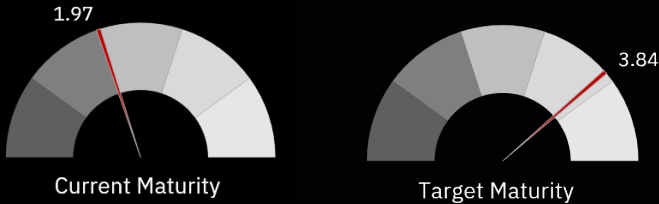
- <client> to understand inherent risks, recoverability, exposure and liabilities; Build specific capabilities to complement the existing operating model to effectively respond to cyber outbreaks

# Management Dashboard



| Cyber Resiliency Phases | Current Maturity Level | Desired Maturity Level | Comments/ Findings                                                                                                                                                                                                                                 | Recommendations                                                                                                                                                                                                                                                                                                                                                |
|-------------------------|------------------------|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identify                |                        |                        | <ul style="list-style-type: none"> <li>Interdependencies between apps &amp; infra is not clearly understood &amp; documented</li> <li>No formal Cyber Resiliency program in place &amp; public relation mechanism not defined</li> </ul>           | <ul style="list-style-type: none"> <li>Create Enterprise baseline &amp; mapping; update periodically</li> <li>Put-in-place a formal Cyber Resiliency Program</li> </ul>                                                                                                                                                                                        |
| Protect                 |                        |                        | <ul style="list-style-type: none"> <li>Currently only data backup is being done. The control files and configuration files are not part of backup</li> <li>Security monitoring is not real time</li> </ul>                                         | <ul style="list-style-type: none"> <li>Ensure the complete data sets are backed-up for critical application</li> <li>Acquire real-time security monitoring capability, Ensure running of Security Operations Center (SOC) 24/7</li> </ul>                                                                                                                      |
| Detect                  |                        |                        | <ul style="list-style-type: none"> <li>Penetration Testing has not been performed for the last 2 years</li> <li>Incident Response plan is not completely updated for inherent cyber risks</li> </ul>                                               | <ul style="list-style-type: none"> <li>Assurance tests must be conducted at least once in a year</li> <li>Update BCP, IRP for inherent cyber risks</li> </ul>                                                                                                                                                                                                  |
| Respond                 |                        |                        | <ul style="list-style-type: none"> <li>Absence for unified communication platform to effectively handle Service continuity</li> <li>Recovery operations currently manual which are prone to human errors &amp; time consuming</li> </ul>           | <ul style="list-style-type: none"> <li>Consider procuring a an unified platform that can help addressing business continuity in real-time that is capable of providing updates e-mail, mobile, social media etc.</li> <li>DR Automation and Orchestration can help reduce dependencies thereby increasing efficiency and provide recovery assurance</li> </ul> |
| Recover                 |                        |                        | <ul style="list-style-type: none"> <li>Recovery objectives are not formally signed-off with the Business</li> <li>Restoration from Backup data is not being tested for all critical apps periodically (Tests are limited to a few apps)</li> </ul> | <ul style="list-style-type: none"> <li>&lt;Client&gt; should consider setting up a formal charter under the Executive Leadership to help align technical architectures with business requirements</li> </ul>                                                                                                                                                   |

# Identify



Táto fáza vytvára základ na to, aby organizácia dokázala prioritizovať úsilie v kybernetickej bezpečnosti v súlade s platnou stratégiou riadenia rizík



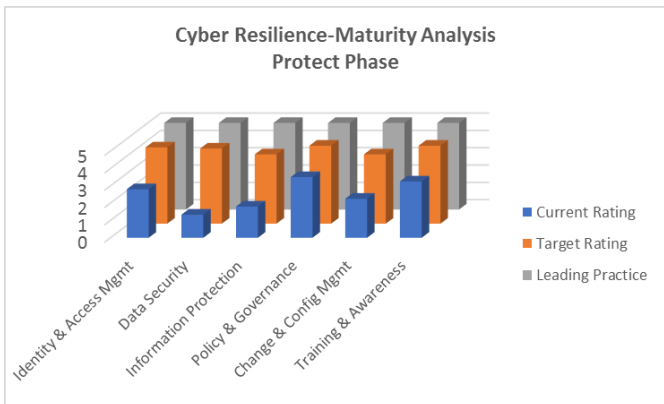
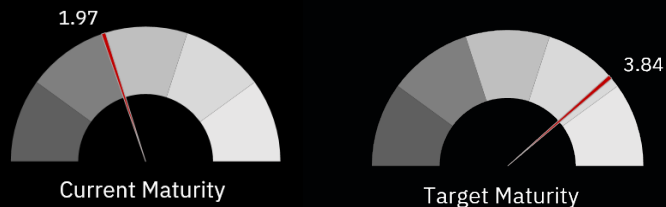
## Cyber Resilience-Maturity Analysis Identify Phase



| Category               | Key Observations / Findings                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organization           | <ul style="list-style-type: none"><li>Need for &lt;client&gt; to formally constitute Cyber Resiliency Program</li></ul>                                                              |
| Technology Environment | <ul style="list-style-type: none"><li>Dependencies must be documented &amp; updated</li></ul>                                                                                        |
| Governance             | <ul style="list-style-type: none"><li>Exposure in terms of Liability (legal, regulatory, 3<sup>rd</sup> party, etc.) with respect to cybersecurity is not fully determined</li></ul> |
| Asset Management       | <ul style="list-style-type: none"><li>Asset Management is at par with the industry standards</li></ul>                                                                               |
| Risk Management        | <ul style="list-style-type: none"><li>&lt;client&gt;'s organization Risk Management to encompass risks arising out of cyber threats</li></ul>                                        |
| Cyber Security Program | <ul style="list-style-type: none"><li>Need for &lt;client&gt; to formally constitute Cyber Resiliency Program</li></ul>                                                              |

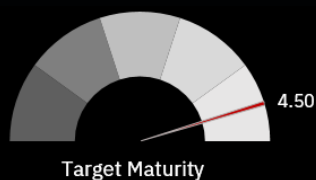
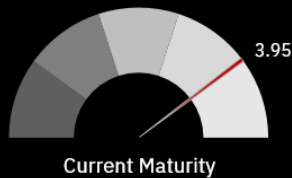
# Protect

Táto fáza napomáha organizácii obmedziť, alebo znížiť dopady a straty spôsobené kybernetickými útokmi



| Category                     | Key Observations / Findings                                                                                                                                                                                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identity & Access Management | <ul style="list-style-type: none"> <li>Good practices covering the enterprise</li> </ul>                                                                                                                               |
| Information Protection       | <ul style="list-style-type: none"> <li>Information protection is well understood &amp; practices</li> </ul>                                                                                                            |
| Policy & Governance          | <ul style="list-style-type: none"> <li>BCP &amp; IRP need updating specific to cyber threats</li> </ul>                                                                                                                |
| Change & Config Management   | <ul style="list-style-type: none"> <li>Good practices covering the enterprise</li> </ul>                                                                                                                               |
| Training & Awareness         | <ul style="list-style-type: none"> <li>&lt;client&gt; to consider rolling out enterprise-wide training /awareness programs specifically around cyber security covering internal stakeholders &amp; partners</li> </ul> |

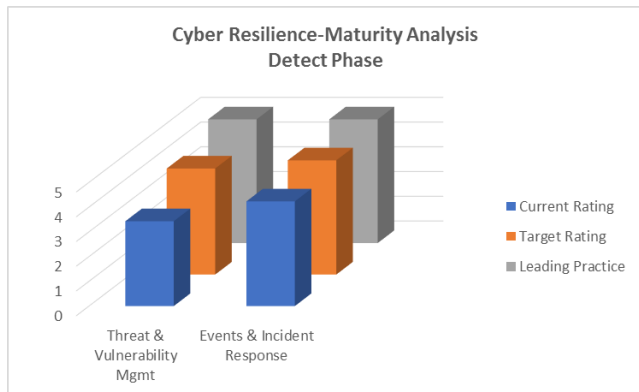
# Detect



Táto kritická funkcia umožňuje organizácii odhaliť anomálie ktoré nastali pôsobením potenciálneho kybernetického útoku



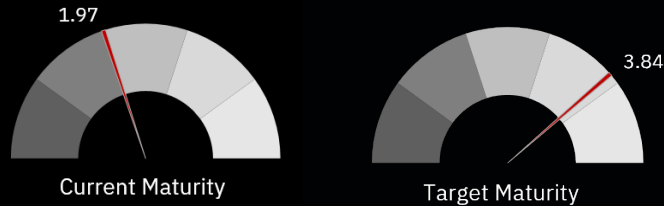
Cyber Resilience-Maturity Analysis  
Detect Phase



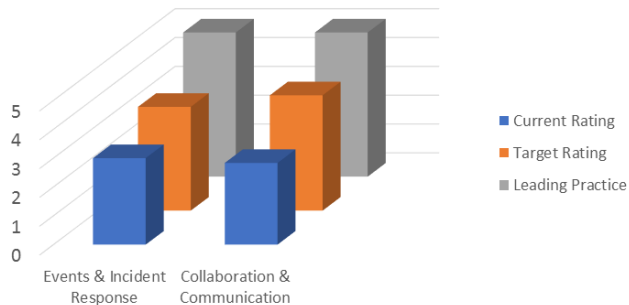
| Category                          | Key Observations / Findings                                                                                                                                                         |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Threat & Vulnerability Management | <ul style="list-style-type: none"> <li>Process for detection of malicious codes must be developed, tested</li> <li>Scope for improvement in terms of Threat intelligence</li> </ul> |
| Events & Incident Response        | <ul style="list-style-type: none"> <li>IRP to be updated for cyber risks</li> </ul>                                                                                                 |

# Respond

V rámci tejto fázy organizácie implementujú sériu primeraných opatrení s cieľom znížiť, alebo obmedziť dopady detegovaných kybernetických útokov



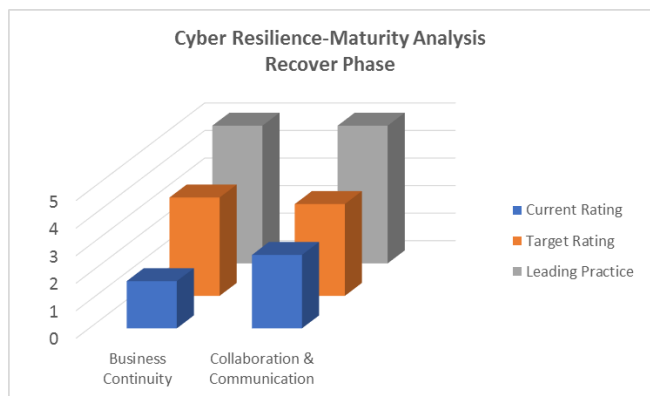
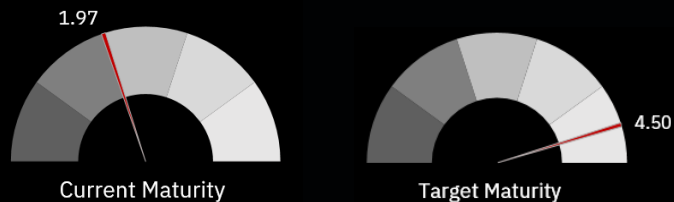
Cyber Resilience-Maturity Analysis  
Respond Phase



| Category                      | Key Observations / Findings                                                                                                                                                                         |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Events & Incident Response    | <ul style="list-style-type: none"> <li>IRP to be updated for cyber risks</li> </ul>                                                                                                                 |
| Collaboration & Communication | <ul style="list-style-type: none"> <li>Current platform relies mostly on phone calls. &lt;client&gt; may consider acquiring an integrated platform for communication during the exigency</li> </ul> |

# Recover

Organizácie v tejto fáze obnovujú svoje činnosti do bežného stavu.



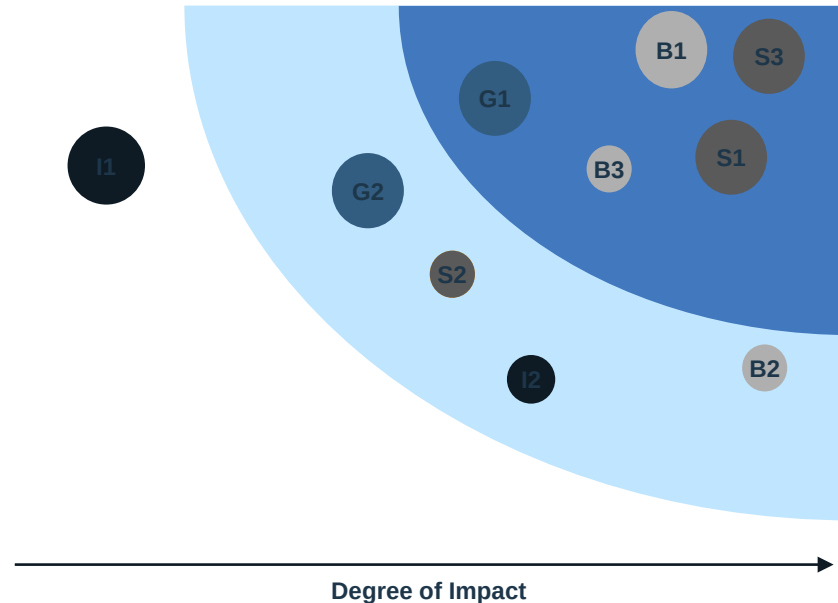
| Category                      | Key Observations / Findings                                                                                                                                                                                                                                                  |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Business Continuity           | <ul style="list-style-type: none"> <li>Recovery Objectives are not mutually signed-off between IT &amp; Business</li> <li>Recovery architectures are not fully aligned to objectives</li> <li>Preparedness in terms of recovery need to be rehearsed periodically</li> </ul> |
| Collaboration & Communication | <ul style="list-style-type: none"> <li>Need for an integrated platform for communication to effectively recover within stipulated time as defined in the recovery plan</li> </ul>                                                                                            |

# Opportunity prioritization matrix

## <Opportunities>

- Are specific initiatives that <client> should pursue based on one/more of our Recommendations
- Modify categories, complexities, impact, etc. based on your assessment
- The graph provides Risk Vs Reward for the opportunities

Degree of Integration



- B Business Resilience**
  - B1 Cyber Resilience Program
  - B2 Recoverability Assessment
  - B3 Automate Recovery
- S Security**
  - S1 24/7, Real Time Monitoring
  - S2 Updating IRP
  - S3 Enhance Threat Intelligence
- I Infrastructure & Systems**
  - I1 Enterprise Blueprinting
  - I2 Build Emergency Communication Platform
- G IT Governance**
  - G1 Cyber Risk Management
  - G2 Training & Awareness
- Complexity**
  - H
  - M
  - L





# Opatrenia na zaručenie kybernetickej odolnosti



# Generické horizontálne rozdelenie opatrení

## – Technické

- opatrenia na zníženie bezpečnostných rizík pomocou prostriedkov fyzickej a technologickej povahy



## – Organizačné

- opatrenia na zníženie bezpečnostných rizík pomocou zmien procesov a úpravou dokumentácie



**Efektívnu bezpečnosť je možné dosiahnuť  
LEN POMOCOU KOMBINÁCIE  
rôznych technických a organizačných opatrení**

# Bezpečnostná architektúra

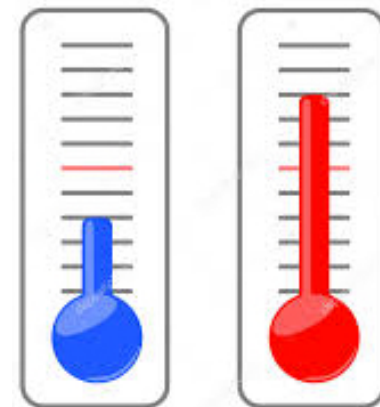
- **Informačná architektúra** - je vo všeobecnosti dizajn podniku, štruktúry a pomenovania častí procesov, systémov, sietí a softvéru s cieľom podporiť čo najlepšiu použiteľnosť.
- „**Bezpečnostná architektúra**“ = vymedzenie okolia informačného systému a jeho vzťah k možnému narušeniu bezpečnosti.
- **Sherwood Applied Business Security Architecture (SABSA)**



|                         | Aktívum<br>(Čo)               | Motivácia<br>(Prečo)            | Proces<br>(Ako)                                 | Ľudia<br>(Kto)                                              | Umiestnenie<br>(Kde)                            | Čas<br>(Kedy)                                         |
|-------------------------|-------------------------------|---------------------------------|-------------------------------------------------|-------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------|
| <b>Kontext</b>          | Predmet činnosti              | Model rizika                    | Model Procesu                                   | Organizačné usporiadanie                                    | Geografia                                       | Časové závislosti obchodnej činnosti                  |
| <b>Koncept</b>          | Profil činnosti               | Bezpečnostné ciele              | Bezpečnostná stratégia a architektonické vrstvy | Model bezpečnostných entít a stanovenie dôveryhodného rámca | Model bezpečnostných domén                      | Termíny a životnosť prvkov súvisiacich s bezpečnosťou |
| <b>Logické členenie</b> | Model informácií              | Bezpečnostné politiky           | Služby bezpečnosti                              | Schéma entít a profily právomocí                            | Definícia bezpečnostných domén a ich prepojenia | Cyklus bezpečnostného spracovania                     |
| <b>Fyzické členenie</b> | Dátový model                  | Bezpečnostné štandardy          | Bezpečnostné mechanizmy                         | Používatelia, aplikácie a používateľské rozhrania           | Platformy a sieťová infraštruktúra              | Výkon riadiacej štruktúry                             |
| <b>Komponenty</b>       | Detailné dátové štruktúry     | Bezpečnostné procedúry a návody | Bezpečnostné produkty a nástroje                | Identity, funkcie, role, ACL                                | Procesy, uzly, adresy, protokoly                | Časovanie a postupnosť bezpečnostných aktivít         |
| <b>Prevádzka</b>        | Zaistenie kontinuity činností | Riadenie operačného rizika      | Riadenie a podpora služieb bezpečnosti          | Riadenie a podpora používateľov a aplikácií                 | Bezpečnosť objektov, sietí a platforiem         | Rozvrh výkonu bezpečnostných operácií                 |

# Ako sa nestat' uvarenou žabou...?

- Priebežne sledujte a vyhodnocujte úroveň informačnej bezpečnosti v organizácii
- Pre dosiahnutie konsolidovaných výstupov stanovte vopred jednoznačnú metriku (KPI, KRI)
- Dobrá prax ukazuje, že meranie bezpečnosti sa dá vhodne vykonávať prostredníctvom merateľných údajov, napr.:
  - číselne vyjadrenej hodnoty rizík (KRI)
  - číselne vyjadrenej úrovne vyspelosti procesov (CMMI)
- Nie je potrebné vynášť koleso.
  - Oprite sa o niektorý z jestvujúcich formálnych rámcov
  - Je účelné použiť rokmi otestované a v praxi overené rámce (ISO27001, ISO22301, NIST, PCI-DSS, COBIT...)
- Organizačné opatrenia sú dôležité, ale papier vám ochranu pred kybernetickým útokom nezabezpečí



# ĎAKUJEM

SLEDUJTE NÁS NA:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

 [ivan.makatura@sk.ibm.com](mailto:ivan.makatura@sk.ibm.com)

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.