

Webinář: RANSOMWARE

Úvodní slovo – uvedení do problematiky

Luděk Novák

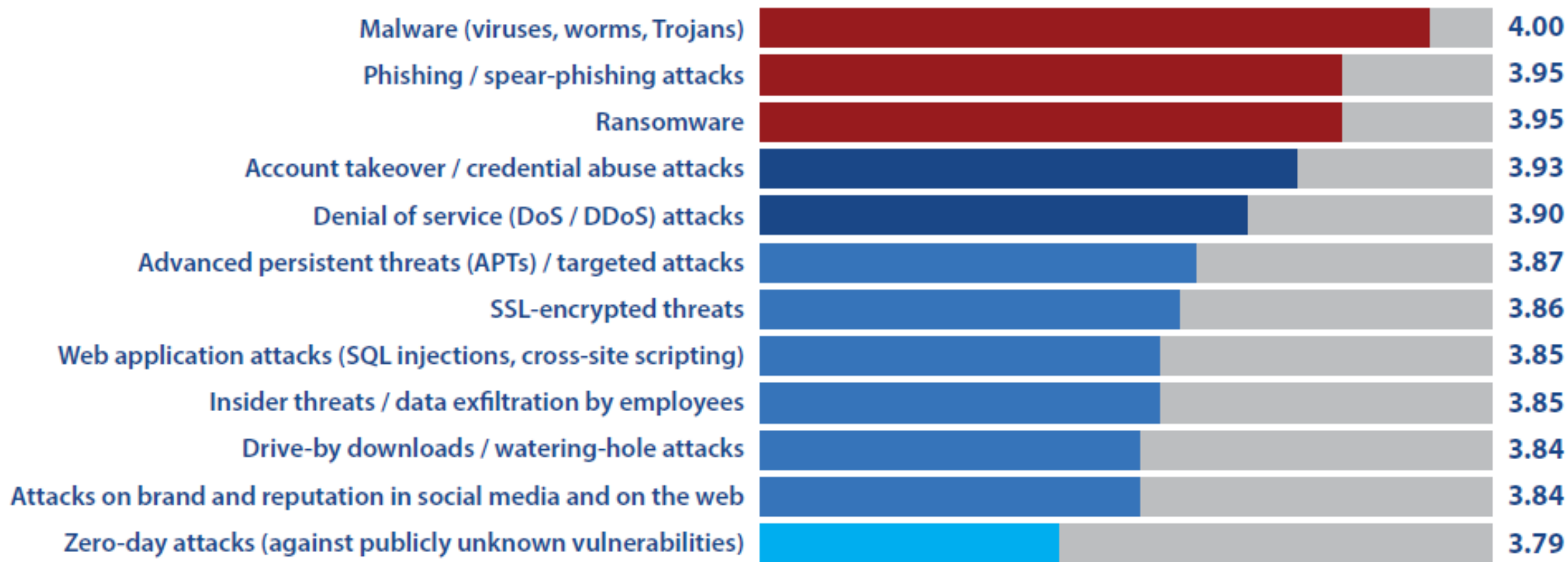
pracovní skupina kybernetické bezpečnosti

Ransomware

- jiné názvy: **vyděračský software, vyděračský program;**
- složení anglických slov *ransom* „výkupné“ a *software*
- druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná, a pak požaduje od oběti výkupné za obnovení přístupu. Některé formy ransomware šifrují soubory na pevném disku (kryptovirální vydírání), jiné jen zamknou systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení.

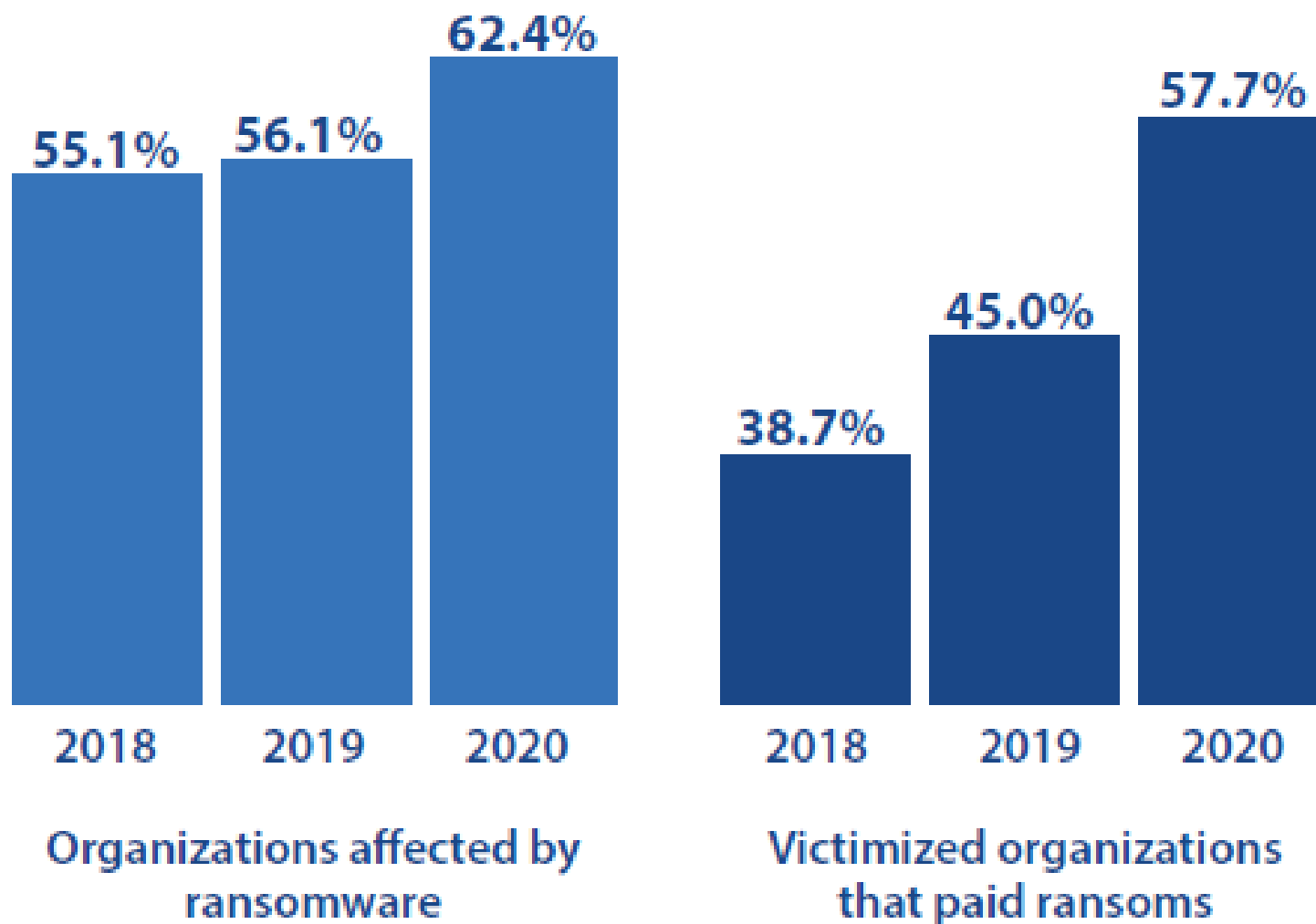
zdroj: <https://cs.wikipedia.org/wiki/Ransomware>

Aktuální statistiky a trendy (I)



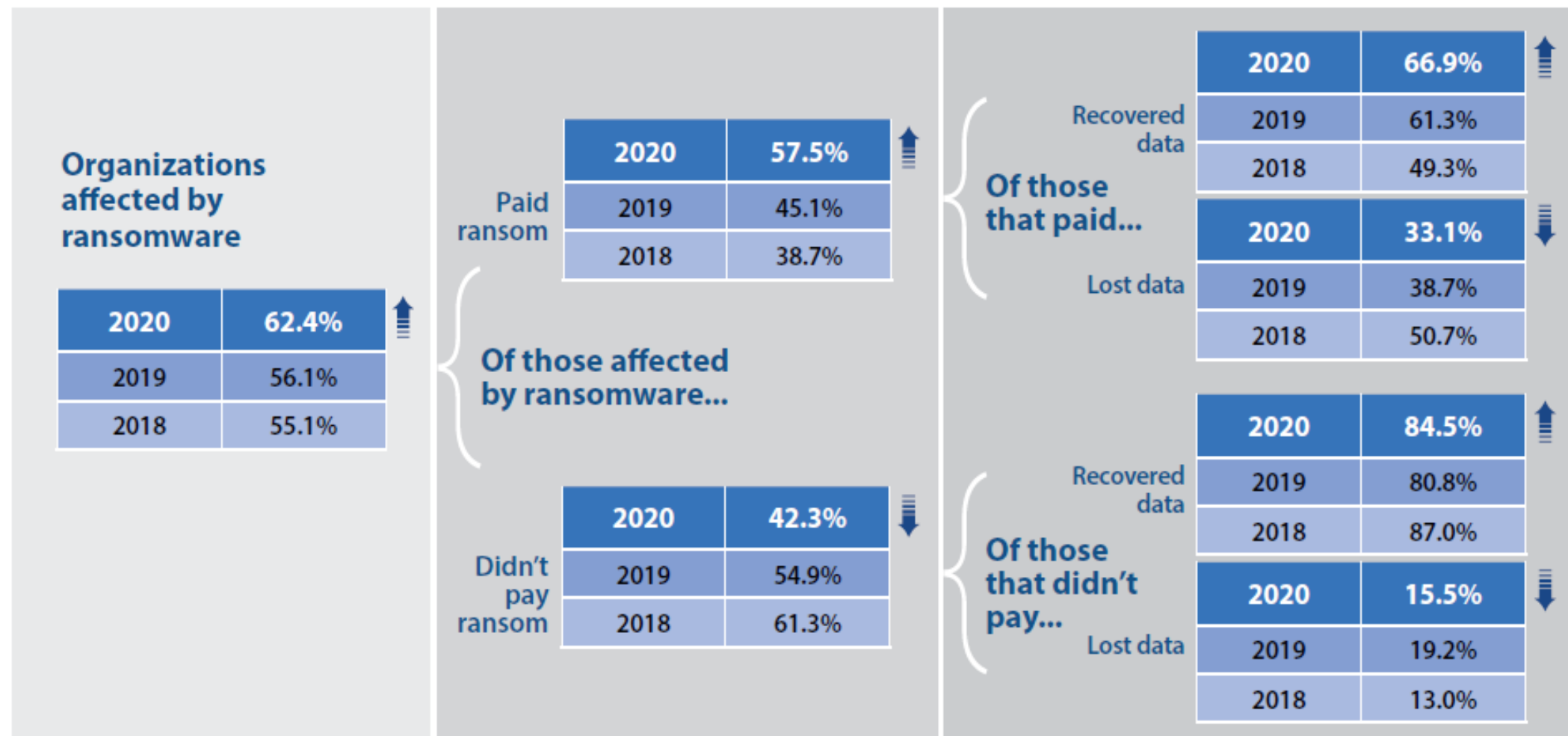
zdroj: <https://cyber-edge.com/cdr/>

Aktuální statistiky a trendy (II)

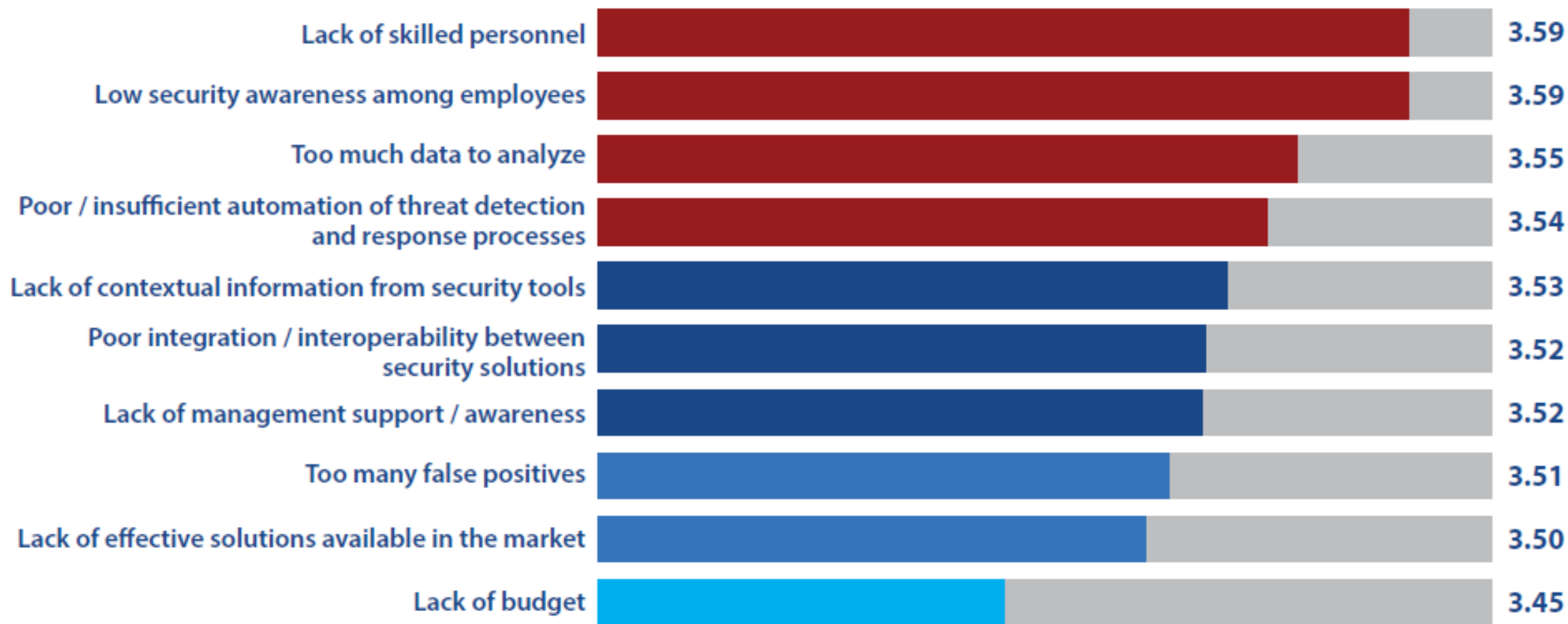


zdroj: <https://cyber-edge.com/cdr/>

Aktuální statistiky a trendy (III)



Aktuální statistiky a trendy (IV)



zdroj: <https://cyber-edge.com/cdr/>

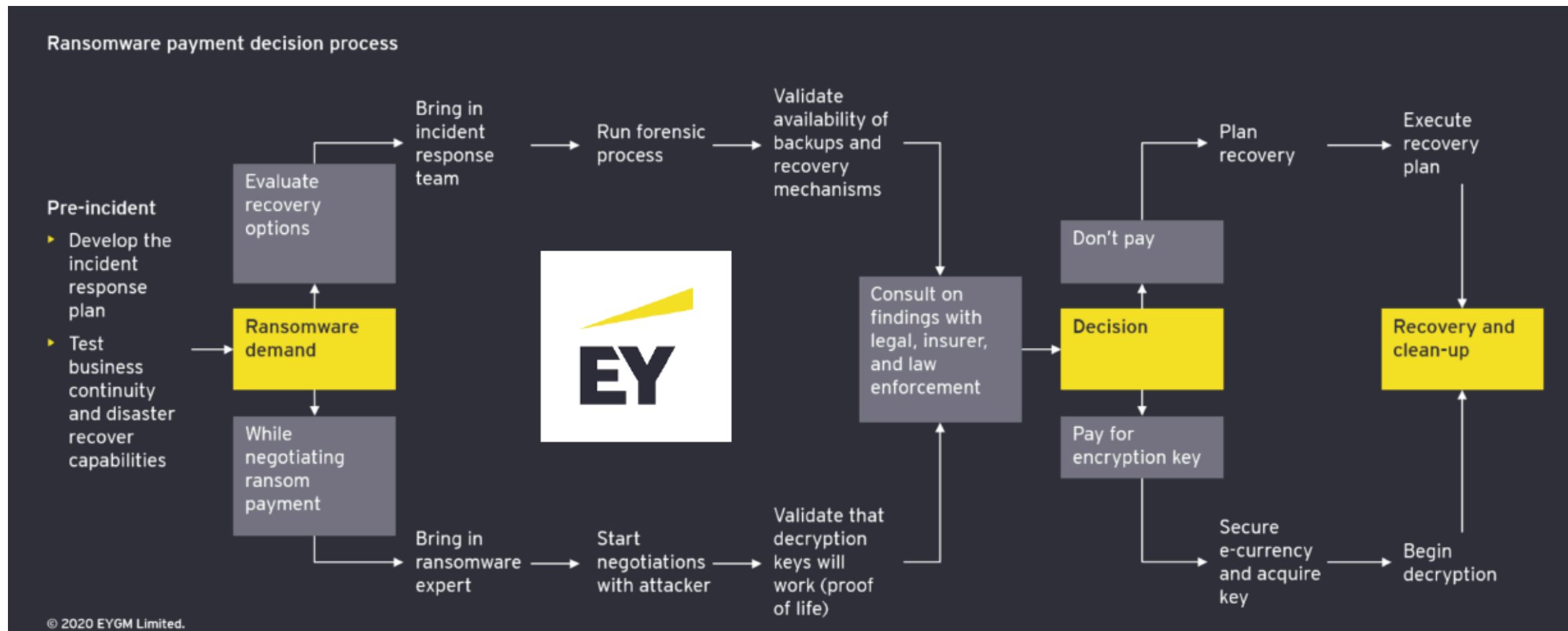
Výzvy spojené s rozhodováním (I)

Decisions by U.S. Cities

- Paid Ransom
 - Lake City, Florida: Paid \$460,000
 - Riviera Beach, Florida: Paid \$600,000
 - Jackson County, Georgia: Paid \$400,000
- Did Not Pay Ransom
 - Atlanta: Spent \$17M to avoid \$51,000 ransom
 - Baltimore: Spent \$18M to avoid \$80,000 ransom
 - New Bedford, MA: Spent \$400K to avoid \$5.3M ransom



Výzvy spojené s rozhodováním (II)



zdroj: <https://www.isc2.org/News-and-Events/Webinars/Security-Briefing>

Výzvy spojené s rozhodováním (III)

Platit

- Kratší výpadek
- Vyšší pravděpodobnost obnovení dat
- Omezení nežádoucí publicity
- **Financování kriminality**

Neplatit

- Řada nákladů spojených s řešením výpadku
- Riziko neobnovení dat
- Riziko nežádoucí publicity
- **Vyšší náklady
(cca 5 – 10x vyšší než výpalné)**

Shrnutí a doporučení

- Prevence
 - Osvědčené metody: **záplaty, zálohy, znalosti**
 - Pokročilé nástroje: 2FA, PAM, NAC, EDR
- Úspěšné zvládání nouzových situací
 - Plány kontinuity IT služeb
 - Testy obnovy IT služeb a dat
 - Efektivní rozhodování na základě objektivních informací