Fort

Radiografia securității cibernetice în România în 2026

Cum se pregătesc organizațiile pentru riscurile cibernetice?

Fort

FORT Cybersecurity, împreună cu Promocrat și DataDiggers, companie românească de cercetare de piață cu experiență în proiecte locale și internaționale, a realizat în perioada **mai–iulie 2026** un studiu despre modul în care organizațiile din România se raportează la securitatea cibernetică: **ce măsuri au implementat, cât de pregătite sunt să facă față unui incident real și ce își propun pentru perioada următoare.**

La cercetare au participat peste **200** de respondenți, majoritatea implicați direct în conducerea organizațiilor sau în deciziile privind securitatea cibernetică. Studiul acoperă măsurile tehnice existente, capacitatea de a identifica și gestiona incidente, pregătirea angajaților, bugetele, utilizarea inteligenței artificiale și stadiul pregătirii pentru NIS2 și DORA.

Fort

Cuprins

Fort

1. Principalele rezultate

Fort

1.1. Multe organizații au măsuri de securitate, dar doar una din patru este pregătită să gestioneze un incident

45% dintre organizațiile participante la studiu s-au încadrat în categoria cu cel mai ridicat nivel de maturitate cibernetică.

Pentru evaluare am folosit un **Indice de Maturitate Cibernetică**, cu valori de la **0** la **100**, care arată cât de bine este pregătită o organizație să prevină, să identifice și să gestioneze riscurile și incidentele de securitate. Indicele ia în calcul cinci componente:

- **Guvernanța securității cibernetice** – cine decide, cine răspunde și după ce reguli;
- **Monitorizarea sistemelor** – capacitatea de a observa la timp că se întâmplă ceva anormal;
- **Capacitatea de răspuns la incidente** – existența unui plan și a oamenilor care îl pun în practică;
- **Igiena tehnică** – măsurile tehnice de protecție implementate: antivirus și firewall, autentificarea multifactor (confirmarea identității printr-un pas suplimentar, pe lângă parolă), copiile de siguranță ale datelor și altele asemenea;
- **Cultura de securitate** – cât de mult este securitatea o preocupare a întregii organizații, nu doar a departamentului IT.

Cele cinci componente au pondere egală în scorul final. În funcție de rezultat, organizațiile au fost împărțite în patru segmente: **Vulnerabil**, **Bazic**, **Gestionat** și **Matur**. Primele două segmente reunesc **34%** dintre organizațiile participante, segmentul Matur **45%**, iar restul de **21%** se încadrează în segmentul Gestionat.

Încadrarea celor **45%** dintre companii în segmentul **Matur** se bazează pe răspunsurile oferite de participanți despre măsurile de securitate pe care organizațiile lor le au implementate. Maturitatea „verificată” scade însă la **27%** atunci când analizăm dacă organizațiile au simultan trei măsuri concrete: monitorizare permanentă, un plan de răspuns testat și exerciții regulate de securitate.

Diferența dintre cele două cifre este importantă:

39 de organizații încadrate inițial în segmentul Matur nu îndeplinesc simultan cele trei criterii practice analizate.

Cu alte cuvinte, instalarea unor soluții de securitate și existența unor proceduri scrise nu sunt suficiente. O organizație pregătită trebuie să poată identifica rapid un incident, să știe cum să reacționeze și să fi verificat, înainte de o situație reală, dacă planul de răspuns chiar funcționează.

1.2. Organizațiile mai bine pregătite identifică și raportează mai multe incidente

15% dintre respondenți spun că organizația lor s-a confruntat cu cel puțin un incident de securitate cibernetică în 2025.

La prima vedere, poate părea surprinzător că procentul este mai mare în rândul organizațiilor cu un nivel ridicat de maturitate: **22%**, față de doar **4%** în cazul celor din categoria vulnerabilă.

Rezultatul nu înseamnă că organizațiile mai bine pregătite sunt atacate de **5,5** ori mai des, ci că identifică și raportează de **5,5** ori mai multe incidente.

La polul opus, 36% dintre organizațiile din segmentul Vulnerabil nu pot estima nici măcar în cât timp ar detecta un incident.

Același lucru se vede în cazul **phishingului** – mesaje frauduloase prin care angajații sunt păcăliți să ofere date sau acces. Organizațiile care fac traininguri de securitate cel puțin trimestrial raportează incidente de phishing în proporție de **14,6%**, față de **1,9%** în cazul celor care nu fac astfel de traininguri. Studiul nu demonstrează că instruirea este cauza acestei diferențe, ci arată că organizațiile care își pregătesc periodic angajații observă mai des problemele.

Concluzia practică: **un număr mic de incidente raportate** nu înseamnă neapărat că **o organizație este mai sigură.** Poate însemna pur și simplu că o parte dintre **incidente trec neobservate.**

1.3. Organizațiile bine pregătite continuă să investească, iar cele slab pregătite riscă să rămână în urmă

Nivelul de pregătire se vede foarte clar în planurile de **buget pentru 2026.**

54% dintre organizațiile cu un nivel ridicat de maturitate spun că își vor crește bugetul pentru securitate cibernetică în 2026. Situația este foarte diferită în segmentul Vulnerabil: doar 4% anticipează o creștere a bugetului, iar pentru 56% bugetul nu era încă stabilit la momentul cercetării.

Organizațiile mature, deja bine pregătite, tratează **securitatea ca pe o investiție continuă.** În schimb, puține dintre organizațiile vulnerabile, care pornesc de la un nivel scăzut de pregătire, intenționează să aloce resurse suplimentare, ceea ce riscă să mărească în timp distanța dintre cele două categorii.

1.4. Pregătirea angajaților este principala prioritate pentru 2026, înaintea tehnologiei

Întrebați care sunt prioritățile de securitate cibernetică pentru 2026, respondenții pun pe primul loc **instruirea angajaților, menționată de 52%.** Urmează **monitorizarea continuă (44%), securitatea AI (41%), securitatea cloud (35%), modernizarea tehnologiei (30%), organizarea internă și stabilirea responsabilităților (24%) și pregătirea pentru noile cerințe legislative (23%).**

Importanța instruirii se confirmă și atunci când respondenții pot răspunde liber, fără variante prestabilite: instruirea și conștientizarea angajaților sunt cel mai frecvent menționate, reprezentând **25% dintre răspunsurile valide.**

Dincolo de investițiile în tehnologie, companiile văd, așadar, pregătirea propriilor oameni drept una dintre principalele condiții pentru **îmbunătățirea securității cibernetice.**

1.5. Inteligența artificială este folosită aproape peste tot, dar puține organizații au reguli pentru ea

94% dintre organizațiile participante declară că folosesc instrumente AI într-o formă sau alta. Utilizarea a devenit, practic, generalizată.

Regulile nu au ținut însă pasul: doar **37%** dintre organizații au politici scrise privind **folosirea AI**, comunicate angajaților. În plus, **48%** dintre respondenți spun că organizația lor are un **control limitat sau nu are deloc control** asupra instrumentelor AI folosite de angajați.

Riscul este deja conștientizat: aproape **70%** dintre respondenți sunt preocupați de posibilitatea ca angajații să introducă informații sensibile ale companiei în instrumente AI.

Există așadar o diferență clară între viteza cu care organizațiile au adoptat AI și capacitatea lor de a gestiona în siguranță utilizarea ei.

Fort

2. Rezultatele în detaliu

2.1. Ce înțeleg companiile prin securitate cibernetică

Majoritatea respondenților văd securitatea cibernetică dincolo de simpla instalare a unor soluții tehnice.

86% consideră că securitatea presupune identificarea vulnerabilităților înainte ca ele să fie exploatate, 83% subliniază instruirea constantă a angajaților, iar 77% spun că securitatea este responsabilitatea fiecărui angajat, nu doar a departamentului IT.

Persistă totuși și unele confuzii despre ce înseamnă, de fapt, securitatea cibernetică: **56%** dintre respondenți au asociat-o și cu achiziționarea celor mai performante soluții antivirus, ca garanție a protecției, iar **13%** cu monitorizarea productivității angajaților.

2.2 Măsurile tehnice există, dar securitatea rămâne, în cea mai mare parte, treaba IT-ului

Măsurile tehnice de bază sunt răspândite în majoritatea organizațiilor participante:

84% folosesc antivirus sau firewall pe toate dispozitivele, 82% folosesc autentificarea multifactor, iar 81% fac periodic copii de siguranță ale datelor și le testează.

Companiile își pregătesc și angajații pentru situații concrete:

74% fac instruire pentru recunoașterea tentativelor de phishing, iar 79% au un canal prin care angajații pot raporta incidentele.

Implicarea restului organizației rămâne însă redusă. Doar **56%** dintre respondenți spun că managementul este vizibil implicat în securitatea cibernetică, iar numai **31%** au persoane desemnate în diferite echipe care să susțină practicile de securitate – cea mai rar întâlnită practică din tot studiul, deși implementarea ei nu presupune investiții semnificative în tehnologie.

Contrastul este clar: măsurile tehnice analizate sunt implementate de **70%** până la **84%** dintre organizații. Când securitatea presupune însă implicarea managementului și asumarea unor responsabilități și în afara echipei IT, procentele scad până la **31%.**

Cu alte cuvinte, s-au făcut progrese la nivel de tehnologie și de instruire, dar securitatea cibernetică este rareori tratată ca o responsabilitate a întregii organizații, de la conducere până la echipele din afara IT-ului.

2.3. Multe organizații au măsuri de securitate, dar puține le testează în practică

Diferența dintre a avea măsuri de securitate și a verifica dacă acestea funcționează în practică se vede în date:

15% dintre organizațiile participante la studiu au implementat opt sau nouă dintre cele nouă măsuri tehnice analizate, dar nu și-au testat niciodată planul de răspuns.

O companie poate avea, așadar, soluții de securitate și proceduri, fără să știe cu certitudine dacă acestea vor funcționa în cazul unui incident real. Pentru asta este nevoie de monitorizare, de un plan clar de răspuns și, mai ales, de testarea lui înainte de apariția unei situații reale.

Organizațiile mai digitalizate au și scoruri mai mari de maturitate: cele care folosesc cloud și AI au un scor mediu de **78**, comparativ cu **44** în cazul organizațiilor cu un nivel minim de digitalizare. Datele arată o legătură între digitalizare și maturitate cibernetică în rândul participanților, fără a demonstra însă că digitalizarea aduce, prin ea însăși, un nivel mai bun de securitate.

2.4. Cu cât o organizație are mai multe resurse IT, cu atât este mai bine pregătită

Cele mai ridicate scoruri de maturitate apar în organizațiile cu echipe IT interne: **80 de puncte.** Organizațiile care folosesc un model mixt, cu personal IT intern și suport extern, au un scor mediu de **73**, iar cele care au externalizat integral serviciile IT către o companie specializată, un scor mediu de **64.**

La polul opus, scorul scade la 52 în cazul organizațiilor care se bazează pe un singur angajat IT și la 33 în cazul celor fără personal IT dedicat – cele mai mici valori dintre toate modelele analizate.

Un rezultat care atrage atenția apare în cazul organizațiilor care se bazează pe un singur angajat IT: niciuna dintre cele **22 de organizații** din această categorie nu a raportat incidente. Acest lucru nu înseamnă neapărat că nu au fost atacate. În contextul scorurilor mai reduse de maturitate ale acestui grup, rezultatul poate indica o capacitate mai redusă de a identifica incidentele atunci când se produc.

Studiul nu arată însă că simpla existență a unei echipe IT interne garantează un nivel mai bun de securitate. Dimensiunea companiei, bugetele și complexitatea infrastructurii influențează atât resursele IT disponibile, cât și nivelul de pregătire.

2.5. Companiile își supraestimează uneori capacitatea de a reacționa la incidente

53% dintre respondenți consideră că organizația lor poate detecta un incident cibernetic semnificativ în mai puțin de 24 de ore, iar 55% cred că poate răspunde eficient într-un interval similar.

Măsurile pe care le au implementate efectiv arată însă o diferență între percepție și nivelul de pregătire. Dintre cei care cred că ar detecta un incident în mai puțin de 24 de ore, **9%** nu au niciun sistem de monitorizare. Iar dintre organizațiile care consideră că ar putea răspunde în mai puțin de 24 de ore, **16%** nu au niciun plan de răspuns la incidente.

Această diferență este cu atât mai importantă în cazul organizațiilor care folosesc aplicații critice, adică aplicații de care depinde direct funcționarea businessului. **72% dintre organizațiile participante folosesc astfel de aplicații**, iar dintre acestea **34%** nu au monitorizare permanentă și **49%** nu au un plan de răspuns testat. Încrederea în capacitatea de reacție nu este, prin urmare, întotdeauna susținută de măsurile existente.

2.6. AI este deja folosit pe scară largă, dar regulile lipsesc

Modul în care este folosit AI-ul diferă mult de la o organizație la alta:

49% îl folosesc oficial pentru anumite sarcini, fără o integrare extinsă, 30% spun că tehnologia este deja integrată la scară largă în procese, iar în alte 15% dintre organizații angajații folosesc instrumente AI pe cont propriu, fără o implementare oficială.

Dincolo de organizațiile care au politici scrise, **25%** au doar reguli informale, **21%** nu au nicio regulă, iar **15%** lucrează în prezent la elaborarea lor.

Lipsa regulilor se reflectă și în nivelul de control: **36%** dintre respondenți spun că au un control limitat asupra instrumentelor AI folosite de angajați, iar **12%** declară că nu există niciun control.

Pe lângă teama de scurgerea informațiilor sensibile, **58%** menționează riscul luării unor decizii pe baza unor răspunsuri incorecte generate de AI, iar **38%** sunt preocupați de probleme legale.

Datele arată că utilizarea AI s-a răspândit mai repede decât regulile și mecanismele prin care organizațiile încearcă să gestioneze riscurile asociate.

2.7. Majoritatea organizațiilor vizate de NIS2 și DORA sunt încă în proces de pregătire

NIS2 și DORA sunt două reglementări europene care impun cerințe de securitate cibernetică: prima pentru organizațiile din sectoare considerate esențiale, a doua pentru sectorul financiar. **41%** dintre organizațiile din eșantion au declarat că sunt vizate de una dintre ele.

Dintre acestea, 29% consideră că îndeplinesc toate cerințele, 14% spun că sunt aproape pregătite, 31% sunt în proces de implementare, iar 14% se află încă în etapa de analiză.

Principalele dificultăți sunt costurile cu tehnologia și consultanța, menționate de **48%** dintre respondenții vizați, și pregătirea documentației și a procedurilor, indicată de **47%.** Stabilirea clară a responsabilităților este o dificultate pentru **34%**, iar lipsa personalului specializat pentru **24%.**

Chiar și în rândul celor 25 de organizații care se consideră complet pregătite apar diferențe între percepție și măsurile implementate: **șase nu fac exerciții regulate de reziliență, iar cinci nu au un plan de răspuns testat.**

Conformitatea nu înseamnă, prin urmare, doar documentație și soluții tehnice. Organizațiile trebuie să fie capabile să aplice în practică măsurile stabilite atunci când apare un incident.

Există și problema inversă. **47% dintre respondenți spun că NIS2 sau DORA nu li se aplică, iar 25 nu știu dacă li se aplică.** Printre cei care se consideră neîncadrați se numără însă șapte organizații din financiar-bancar – sector acoperit aproape integral de DORA – trei din sănătate, trei din transport și două din energie. Cel puțin **15** organizații își clasifică, foarte probabil, greșit obligația legală.

3. Ce spun companiile

Două dintre întrebările studiului au fost deschise: participanții au putut spune liber care sunt principalele probleme cu care se confruntă și ce i-ar ajuta cel mai mult, fără să aleagă dintre variante prestabilite.

Phishingul și ingineria socială sunt cele mai frecvent menționate, în 13% dintre răspunsurile valide, urmate de comportamentul angajaților, cu 12%.

Când sunt întrebați ce i-ar ajuta cel mai mult, respondenții indică în primul rând instruirea angajaților pentru creșterea nivelului de conștientizare a riscurilor. Nevoia de mai mulți **specialiști** sau de un **CISO** – responsabilul pentru securitatea informației la nivel de organizație – **apare în 17% dintre răspunsuri, bugetul și finanțarea în 12%, iar tehnologia sau modernizarea în 10%.**

Este relevant că tehnologia nu apare în fruntea listei. Atunci când descriu cu propriile cuvinte de ce au nevoie, respondenții **menționează mai des oamenii, pregătirea și competențele decât achiziția de echipamente sau software.**

În cazul AI apare o diferență interesantă. Când primesc o listă de priorități pentru 2026, **41% includ securitatea AI între primele trei.** Când sunt întrebați liber despre problemele curente, AI apare în doar **2,4%** dintre răspunsurile valide. AI este, așadar, percepută ca o prioritate pentru viitorul apropiat, dar nu se numără încă printre problemele resimțite ca presante în prezent.

4. Concluzii pe scurt, și despre studiu

Organizațiile participante la studiu au făcut deja **pași importanți în domeniul securității cibernetice.** Majoritatea respondenților înțeleg că securitatea înseamnă mai mult decât instalarea unor soluții tehnice, iar măsurile de bază sunt larg răspândite.

Diferențele apar atunci când analiza trece de la existența măsurilor la modul în care ele sunt **folosite și testate.** Mai puțin o treime dintre organizațiile participante combină monitorizarea permanentă cu un plan de răspuns testat și exerciții regulate, iar încrederea în propria capacitate de reacție este adesea mai mare decât o susțin măsurile existente.

Organizațiile mature identifică și raportează mai multe incidente, ceea ce arată că un număr mic de incidente raportate nu înseamnă neapărat un nivel mai bun de securitate.

Pregătirea angajaților este **principala prioritate pentru 2026.** În cazul AI, utilizarea este deja aproape generalizată, în timp ce **regulile și controlul** asupra modului în care este folosit au nevoie de îmbunătățiri.

Securitatea cibernetică nu depinde numai de tehnologia pe care o organizație o are la dispoziție. **Capacitatea de a identifica un incident, de a reacționa, de a testa periodic procedurile și de a pregăti oamenii este cel puțin la fel de importantă.**

În același timp, organizațiile deja bine pregătite sunt și cele care intenționează cel mai frecvent să își **crească investițiile în securitate**, în timp ce cele vulnerabile **alocă rar resurse suplimentare.** În timp, acest lucru poate accentua diferențele dintre cele două categorii.

Despre studiu

Studiul a fost realizat de FORT Cybersecurity împreună cu Promocrat și DataDiggers, pe baza unui chestionar structurat aplicat în perioada **mai–iulie 2026.** Chestionarul a avut **32 de întrebări**, iar la el au răspuns peste **200 de persoane.**

5. Cine a răspuns

- **Regiune: 74%** dintre respondenți provin din București-Ilfov.
- **Domenii:** IT și servicii digitale – **35%**; financiar-bancar și asigurări – **14%**; producție și industrie – **10%**; energie și utilități – **8%.**
- **Dimensiunea organizațiilor: 32%** au sub 10 angajați, iar **22%** au peste 1.000 de angajați.
- **Rolul respondenților: 44%** fac parte din conducerea executivă, **19%** ocupă funcții de IT sau tehnologie, iar 10% ocupă poziții de conducere în securitate.

6. Cum au fost prelucrate răspunsurile libere

Răspunsurile la cele două întrebări deschise au fost grupate pe teme. Pentru că un singur răspuns poate menționa mai multe teme, **procentele nu însumează 100%.** Analiza se bazează pe **169 de răspunsuri valide** pentru întrebarea privind provocările și **170** pentru cea privind nevoile. În cazul provocărilor, răspunsurile de tip „fără incidente / nu e cazul", reprezentând **34% din total**, au fost excluse din analiză.

Rezultatele descriu organizațiile care au participat la cercetare și nu sunt reprezentative statistic pentru totalitatea organizațiilor din România. În eșantion sunt suprareprezentate organizațiile din București, cele din sectoarele IT și financiar, precum și decidenții deja implicați în securitate. **Piața în ansamblu este, cel mai probabil, mai puțin pregătită decât indică aceste rezultate.**