Primljeno: 24.06.2021.
Odobreno: 07.10.2021.

DOI: 10.5937/bankarstvo2103140P

SAJBER INCIDENTI POVEZANI SA FINANSIJSKIM INSTITUCIJAMA

Ksenija Popović, doktorand,
Alpen Adria Univerzitet u Austriji
email: ksenijapo@edu.aau.at

Rezime

Osnovna tema rada je ubrzana digitalna transformacija finansijskih institucija koja, pored prednosti, donosi i povećan rizik od sajber incidenata. Sajber incidenti mogu naneti štetu od sistemskog značaja i zato izgradnja dobrog sistema sajber bezbednosti prevazilazi okvire pojedinačnih finansijskih institucija. Na osnovu uporedne analize trenda svesti javnosti o sajber napadima, zaključak ovog rada je da za razliku od razvijenih zemalja, svest javnosti u Srbiji nema kontinuiran nego povremen rast izazvan pojedinačnim događajima povezanim sa sajber napadima. Dizajniranje nacionalne kampanje za podizanje svesti javnosti o sajber bezbednosti, kao i obučavanje i zadržavanje visokokvalifikovanih kadrova dve su preporuke koje se same nameću nakon opservacije i analize informacija o sajber incidentima u Srbiji.

Ključne reči: Zlonamerni sajber incident; digitalna transformacija; finansijske institucije; sajber bezbednost

JEL klasifikacija: G20, K24

Uvod

Grupa G20 je 2017. godine upozorila da sajber incidenti mogu ugroziti stabilnost finansijskog sektora (G20 Communiqué, 2017), te je dodelila zadatak svom Odboru za finansijsku stabilnost da popiše nacionalne regulative i primere dobre prakse u vezi sa sajber incidentima. Zemlje članice G20 proizvode 80% svetskog BDP-a, a u njima živi 60% svetske populacije. U aprilu 2020. godine pomenuti Odbor za finansijsku stabilnost je objavio preporuke finansijskim institucijama šta raditi pre, za vreme i nakon sajber incidenta (G20 Financial Stability Board, 2020). Odbor za finansijsku stabilnost je jačanje otpora na sajber napade takođe postavio među prioritetne zadatke u svom programu za 2021. godinu (G20 Financial Stability Board, 2021).

Kristin Lagard, predsednica Evropske centralne banke, upozorila je u februaru 2020. godine da bi dobro organizovan sajber incident na glavne finansijske institucije mogao izazvati ozbiljnu finansijsku krizu (Thornton, 2020). A u isto vreme, Evropski odbor za sistemski rizik, zadužen za makroprudencijalni nadzor u EU, objavljuje izveštaj Sistemski sajber rizik. U ovom izveštaju piše: „...nije nezamislivo da bi u budućnosti veliki sajber incident u finansijskom sektoru mogao stvoriti poremećaj tolikog obima da može imati ozbiljne negativne posledice na unutrašnje tržište i realnu ekonomiju“ (European Systemic Risk Board, 2020, str. 23). U aprilu 2021. godine, predsedavajući Federalnih američkih rezervi Džerom Pauel je izjavio da je sajber rizik povezan sa finansijskim institucijama veći i iznad bilo kog drugog rizika u zemlji (Vavra, 2021).

Putem opservacije i analize već postojećih informacija na ovu temu, cilj ovog rada je da odgovori na dva pitanja: prvo, zašto se tolika pažnja usmerava na sajber incidente i drugo, kakva je situacija na finansijskom tržištu Srbije. Struktura rada je sledeća: U prvom delu se navode prednosti i nedostaci tehnološkog progressa u finansijskim institucijama. Definicija sajber incidenta, akteri pretnje, vrste i konkretni primeri sajber incidenata se daju u drugom delu. U trećem delu se definiše sistemski sajber rizik i analiziraju mere za poboljšanje sajber bezbednosti, uključujući i par preporuka za Srbiju.

Digitalna transformacija

Digitalna transformacija obuhvata niz malih i velikih tehnoloških pomaka koje ne samo da pomeraju ponudu ka onlajn i digitalnim uslugama finansijskih institucija, već uključuju i primenu savremene tehnologije u svim sferama rada. U procesu regrutovanja novih radnika, na primer, banke sve češće koriste veštačku inteligenciju da napravi uži izbor kandidata na osnovu ključnih reči iz njihovih biografija. Sa jedne strane, digitalizacija čini interne procese efikasnijim, a sa druge strane, menja način komunikacije sa korisnicima bankarskih usluga. Skoro sve banke sada imaju svoje profile na društvenim mrežama (Facebook, Twitter, LinkedIn...), dok veb-roboti komuniciraju sa korisnicima na platformama za časkanje zahvaljujući veštačkoj inteligenciji. Banke takođe nude digitalno otvaranje računa, instant plaćanja u roku od nekoliko sekundi, usluge u digitalnoj filijali, elektronske keš kredite... E-banking omogućava korisnicima da pristupe svojim računima i koriste ih bilo kad i bilo gde. M-banking omogućava bankama da prodaju svoje proizvode i putem aplikacija za mobilne telefone.

Prema empirijskom istraživanju, u periodu od 1992. do 2014. godine, bankarski sektori zemalja evrozone razvijaju se konvergirajući prema najboljoj dostupnoj tehnologiji, a produktivnost bankarskih sektora raste zahvaljujući stalnim tehnološkim pomacima, mada po sve nižim stopama (Casu, Ferrari, Girardone, & Wilson, 2016). Bankarski sektor Srbije drži korak sa ovim tehnološkim promenama (Zec, 2021), najviše zato što u njemu dominiraju razvijene strane banke.

Na finansijskom tržištu postoji mali broj onih koji su predvodnici tehnološkog razvoja, sa jedne strane, i postoji većina koja prate tržišne lidere nastojeći da smanje tehnološki jaz, sa druge strane. Navodim nekoliko primera napredne digitalne transformacije koju provode velike bankarske grupacije: HSBC grupa, koja je šesta i Bank of Amerika koja je osma najveća bankarska grupacija na svetu prema ukupnoj imovini na kraju 2019. godine (S & P Global Market Intelligence, 2020):

- **Cloud computing** je nova tehnologija koja obezbeđuje internet mesto ili oblak dajući pojedincima i bankama (kao i ostalim kompanijama) mogućnost da koriste resurse, kao što su virtuelne mašine, baze podataka, memorija, usluge, arhiva, slanje poruka, itd. Zbog toga cloud computing doprinosi, pored ostalog, nižim troškovima kompjuterske infrastrukture, boljem izveštavanju i analizi, bržem i lakšem pristupu podacima, boljem uvidu u potencijal unakrsne prodaje. U oktobru 2019. godine, Bank of Amerika je 80% aktivnosti izvršavala preko sopstvenog oblaka, čime je smanjila sa 200.000 na 70.000 broj svojih servera. Bank of Amerika sada namerava da preseli svoje aktivnosti na javni oblak (CapGemini & EFMA, 2021, str. 22). HSBC banka je objavila u julu 2020. godine da je odabrala javni oblak firme Amazon Web Services za svoje poslovne aktivnosti na globalnom nivou (Flinders, 2020).

To internet mesto može biti u sopstvenom vlasništvu ili javno (u tom slučaju domaćin je neko drugi, tj. dobavljač oblaka). Četiri najveća dobavljača oblaka su Amazon Web Services, Microsoft Azur, Google Cloud i Alibaba Cloud. Prema procenama Canalysa (Canalys, 2021), njihovo tržišno učešće u Q4 2020 je dominantno u odnosu na ostale dobavljače (grafika 1). Iako se podaci Canalysa ne odnose samo na potrošnju oblak resursa od strane banaka, jasna je tendencija homogenizacije oko nekoliko najvećih cloud dobavljača.

Grafika 1: Svetska potrošnja infrastrukture oblaka, 39,9 milijardi USD, Q4 2020

Izvor: Canalys (Canalys, 2021).

- HSBC banka učestvuje i u evropskom NEASQC istraživačkom projektu primene **quantum computing tehnologije**. NEASQC je skraćenica za Next Applications of Quantum Computing (u prevodu „Buduće primene kvantum tehnologije“). Smatra se da kvantum kompjuteri imaju veće sposobnosti da obavljaju izuzetno kompleksne zadatke u odnosu na današnje kompjutere (HSBC, 2020).

- **Biometrijska tehnologija** u bankama znači da će se PIN kodovi i lozinke uskoro zameniti biološkim karakteristikama ljudi. HSBS banka je najavila glasovnu verifikaciju svojih klijenata (Grant, 2021).

Čak i naprednije zemlje razmišljaju o novim tehnologijama koje mogu potpuno preokrenuti način rada u budućnosti:

- Na **distributed ledger technology (DLT)** se gleda kao na moguću treću generaciju platnog sistema, nakon generacije zasnovane na papiru i one zasnovane na batch obradi (IMF Fintech Notes 20/01, 2020). Na primer, centralna banka Kanade i monetarne vlasti Singapura bilateralno su povezale svoje eksperimentalne platne sisteme u kojima se koristi digitalni novac. One su povezale dve različite DLT platforme. Drugi primer, SWIFT je kreirao novu GPI platformu radi povećanja brzine plaćanja. Ta platforma nije DLT platforma, ali istražuje se mogućnost da se blokčejn kompanije povežu na SWIFT GPI platformu (IMF Fintech Notes 20/01, 2020). Blokčejn je vrsta DLT platforme.

Sa pojavom pandemije, finansijske institucije pokušavaju da se prilagode promenljivom, neizvesnom i složenom okruženju. Zatvaranja koja su usledila u svim zemljama tokom pandemije korona virusa primorala su banke i ostale finansijske institucije da zatvore svoje filijale, a korisnike da se sve više okrenu onlajn uslugama. Udeo beskontaktnih plaćanja, onlajn plaćanja, plaćanja putem kartica se povećava, dok se udeo plaćanja gotovim novcem smanjuje (Ernst & Young, 2020). Zbog pandemije i veći broj radnika finansijskih institucija počinje da radi od kuće, što znači da zaposleni ne rade više u virtuelnom i fizičkom prostoru pod kontrolom tih finansijskih institucija. Prisustvujemo ubrzanju primene digitalne tehnologije.

Međutim, digitalna transformacija ima i određene nedostatke. Tokom pandemije broj sajber napada na finansijske institucije se toliko uvećao da je finansijski sektor postao druga najčešća meta napada, odmah nakon zdravstvenog sektora (BIS, 2021). Postavlja se pitanje da li finansijski sektor može da drži korak sa rastućim brojem zlonamernih sajber napada.

Sajber incident

Sajber incidenti postaju sve češći, inovativniji, sofisticiraniji, u višestrukim formama dok je sajber rizik tek delimično shvaćen (Kopp, Kaffenberger, & Wilson, 2017). Svaka finansijska institucija je izložena sajber riziku, zato što ne postoji savršen sistem sajber bezbednosti - "neke nepoznate rupe u sistemu uvek postoje bez obzira na tehnološku sofisticiranost" (Uddin, Ali, & Hassan, 2020, str. 9). Ideja mog rada je da se približi tema sajber incidenata, počevši od definicije, aktera i vrsta sajber incidenata.

Prema sajber leksikonu (G20 Financial Stability Board, 2018, str. 9), sajber incident je: „sajber događaj koji:

- ugrožava sajber bezbednost informacionog sistema ili informacija koje sistem obrađuje, čuva ili prenosi; ili
- krši bezbednosne politike, bezbednosne procedure ili politike prihvatljive upotrebe, bilo da proizilazi iz zlonamerne aktivnosti ili ne“.

Sajber incident može dakle biti slučajan ili zlonameran. Ali, ovde nas interesuju prevashodno zlonamerni sajber incidenti, zato što su oni brojniji. Preciznosti radi, razlika između sajber napada i sajber incidenta je u tome što napad prethodi incidentu. Mada, u Srbiji se koristi termin sajber napad da opiše oba događaja, i napad i incident.

Nekoliko je aktera sajber pretnje: nacionalni, kriminalni, teroristički, aktivisti, zaposleni sa različitim motivima (videti tabelu 1). Severna Koreja se često smatra sponzorom sajber grupa koje su uključene u krađe novca, pranje novca i kampanje iznude (Varga, Brynielsson, & Franke, 2021; Cybersecurity & Infrastructure Security Agency, 2020). Sajber kriminalne grupe su ipak najčešći akteri pretnje, a neke od dobro poznatih su Carbanak, Silence, Lazarus, Old-Gremlin i Black Shadow.

Tabela 1:

Akter pretnje	Motivi
Nacionalni	Geopolitički i ideološki
Kriminalni	Sticanje materijalne koristi
Terorističke grupe, hakeri aktivisti	Ideološki, nezadovoljstvo
Interna pretnja	Pohlepa, razočarenje

Izvor: ESRB (European Systemic Risk Board, 2020).

Postoji i više vrsta sajber incidenata, a najčešće vrste uz kratak opis su navedene u tabeli 2. Međutim, ima nekoliko zajedničkih karakteristika različitih vrsta sajber incidenata. Prvo, teško se uočavaju. Istraživanje koje je obuhvatilo finansijske institucije širom sveta u periodu od 2002-2019. god. došlo je do zaključka da je u proseku je potrebno 251 dan od momenta dešavanja do momenta detektovanja gubitaka nastalih po osnovu sajber incidenata (Aldasoro, Gambacorta, Giudici, & Leach, 2020a). Drugo, zbog svoje anonimnosti i ireverzibilnosti transakcija, kriptovalute su se ustalile kao metod plaćanja sajber napadača od strane žrtava napada (EUROPOL, 2020). Treće, finansijske institucije nisu uvek voljne da prijavljuju sajber incidente zbog reputacionog rizika (Britz, 2013; Varga, Brynielsson, & Franke, 2021).

Tabela 2:

Vrsta sajber incidenta	Kratak opis
Malware	Softver dizajniran da nanese štetu (npr. kompjuterski virusi, Trojanci...)
Man-in-the middle	Smeštanje usred transakcije između dve strane
Cross-site scripting	Zloupotreba ranjivosti veb aplikacije, kojoj žrtva, korisnik te aplikacije, inače veruje
Phishing	Oponašanje pouzdanog entiteta u digitalnoj komunikaciji, kako bi se zadobilo poverenje žrtve
Password cracking	Identifikacija nepoznate lozinke
A zero-day exploit	Zloupotreba uočene ranjivosti softvera ili hardvera
Distributed Denial of Service(DDoS)	Višestruki napad na metu (na primer server, internet stranicu ili mrežu) koji onemogućava dalju uslugu korisnicima

Izvor: BIS bilten br. 37 (BIS, 2021) i Aldasoro, Gabacorta, Giudici & Leach (2020b).

Na zvaničnoj internet stranici Carnegie fondacije za međunarodni mir nalazi se baza podataka koja sadrži važnije sajber incidente povezane sa finansijskim institucijama širom sveta (tzv. Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Endowment for International Peace). Carnegie fondacija za međunarodni mir je međunarodni analitički centar, osnovan 1910. godine. Vrste sajber incidenata koje evidentira ova baza su upad u bazu podataka, krađa, špijunaža i prekid rada. Evo nekoliko primera sajber incidenata u svetu:

- U januaru 2021. god., centralna banka Novog Zelanda pretrpela je upad u svoju bazu podataka.
- U decembru 2020. god. izraelska osiguravajuća kompanija bila je pod napadom Black Shadow sajber kriminalne grupe, koja je tražila 200 bitkoina u zamenu za ukradene podatke.
- U septembru 2020. god. nekoliko mađarskih banaka je prekinulo rad zbog DDoS napada.
- U avgustu 2020. god. jedna marokanska banka je pretrpela upad u račune klijenata i neovlašćeno sprovođenje transakcija.
- U martu 2020. god. kriminalna sajber grupa OldGremlin ulazi u mreže nekoliko ruskih banaka, šifrira podatke i traži otkup.

Na osnovu javno dostupne evidencije Nacionalnog CERT Republike Srbije (CERT je akronim za Computer emergency response team), najčešći sajber incidenti povezani sa finansijskim institucijama u našoj zemlji odnose se na maliciozne phishing kampanje usmerene prema klijentima banaka (<https://cert.rs/obavestenja.html#613>). Mediji su u maju 2017. godine preneli da je bio pokušaj da se nanese materijalna šteta Zavodu za izradu novčanica i kovanog novca, koji posluje u okviru Narodne banke Srbije, putem zlonamerne phishing poruke (Tanjug, 2017; BizLife, 2017).

Zapravo svi oni sektori koji su od kritičke važnosti za ekonomiju jedne zemlje, kao što su naftovodi, električno snabdevanje, bankarski sektor, itd., treba da budu predmet nacionalne bezbednosti kada su sajber incidenti u pitanju (Aldasoro, Gambacorta, Giudici, & Leach, 2020b; Brenner, 2017).

Sistemska sajber rizik

Visok je nivo međusobne povezanosti među finansijskim institucijama, a naročito njihovih IT sistema. To doprinosi većoj brzini i širim razmerama prenosa negativnih posledica potencijalnog sajber incidenta. Ali nije svaki sajber incident sistemske prirode. Izveštaj Carnegie fondacije za međunarodni mir predlaže nekoliko konkretnih uslova koji kumulativno treba da budu zadovoljeni za kategorisanje sajber incidenta u sistemska (Brauchle, Göbler, Seiler, & von Busekist, 2020):

- usmerenost ka sistemski važnoj finansijskoj instituciji ili nekoliko finansijskih institucija (funktionalni kanal);
- vreme trajanja incidenta traje 2 sata i/ili je dugo toliko da sprečava poravnanje na kraju dana;
- direktni i indirektni finansijski gubitak prelazi nivo kapitala banke (finansijski kanal);
- gubitak poverenja meren trajanjem vesti o incidentu, brojem uključenih medija i geografski prostor koji pokrivaju (kanal poverenja).

Evropski odbor za sistemske rizike je analizirao nekoliko hipotetičkih sistemskih sajber rizika (European Systemic Risk Board, 2020), među njima: (i) pad sistema plaćanja sistemski važne domaće banke i (ii) brisanje podataka o stanju na računima praćeno neovlašćenim plaćanjima. U oba slučaja, što duže traje sajber napad, to su veće negativne posledice. Opšti gubitak poverenja izaziva sistemski karakter sajber incidenta. „Na primer, ako bi - nakon uspešnog zlonamernog sajber incidenta - klijenti banke utvrdili da su sva stanja na računima nula ili nedostupna duže vreme, te da institucija ne može da reši situaciju u razumnom vremenskom roku, moguće je da bi panika počela da se širi. Kao otežavajući faktor, lažne vesti i dezinformacije u takvom slučaju mogu se širiti putem društvenih mreža, moguće i kao deo incidenta, dodatno destabilišući tržišta i društvo“ (European Systemic Risk Board, 2020, str. 38).

Postoji mišljenje da prenos IT funkcija finansijskih institucija na cloud može biti takođe izvor sistemskog sajber rizika (Danielsson & Macrae, 2019; Aldasoro, Gambacorta, Giudici, &

Leach, 2020b). Obzirom na trend homogenizacije oko najvećih cloud dobavljača, bilo kakav sajber ili neki drugi incident na cloud-u može uticati na više finansijskih institucija u isto vreme. Setimo se požara u martu 2021 godine, kada je od četiri data centra OVH cloud-a u Strazburu, jedan uništen, a drugi oštećen. Milionski broj veb-sajtova bio je van funkcije, uključujući i one od raznih agencija vlade, banaka, novina, radnji, itd. OVH cloud je inače najveći evropski cloud dobavljač. Danielsson i Macrae (2019) predlažu regulisanje poslovanja cloud dobavljača, jer je pitanje da li bi jedan privatni cloud dobavljač dao prioritet klijentima iz svoje ili neke druge zemlje, da li bi dao prioritet vladi ili finansijskim institucijama – u slučaju rešavanja posledica zlonamernog sajber incidenta.

Jedan od važnih zadataka radi povećanja stepena sajber bezbednosti je uvođenje standarda i regulativa na nacionalnom, ali i internacionalnom nivou. Postavljanje standarda i regulative u oblast sajber prostora je važno zato što „se pojedinačne kompanije ne bave u potpunosti izgubljenim poverenjem javnosti u ceo sistem kada neko upadne u podatke njihovih klijenata, zbog čega mogu u sajber bezbednost uložiti manje nego što bi bilo u javnom interesu. Ova briga ima poseban značaj u finansijskom sektoru, gde je održavanje poverenja javnosti ključno“ (Carrière-Swallow & Haksar, 2021, str. 13). Neke centralne banke, kao npr. Centralna banka Francuske, imaju posebne jedinice (The Paris Resilience Group ili le groupe de place Robustesse) posvećene simulaciji raznih šok scenarija, od prirodnih katastrofa do izazvanih kriza kao što je sajber napad. Cilj ovih jedinica je da održi kredibilitet u institucije i pojača otpornost u slučaju velikih operativnih kriza (Donas, 2021).

Obzirom da sajber napadi prevazilaze pojmove fizičkih granica među zemljama, jer se odigravaju u virtuelnom sajber prostoru, veoma je važna međunarodna saradnja i razmena podataka. U novembru 2020. godine, Carnegi fondacija za međunarodni mir i Svetski ekonomski forum objavili su Međunarodnu strategiju za bolju zaštitu globalnog finansijskog sistema od sajber pretnji. U velikom broju zemalja, uključujući i našu, osnovani su CERT timovi koji imaju za cilj da promptno odgovore na eventualne sajber incidente. Podjednako je strateški važna precizna raspodela odgovornosti unutar zemlje, kao i demarkacija nacionalnih jurisdikcija u slučaju sajber napada. Tek nekoliko zemalja sveta ima jasnu raspodelu uloga i odgovornosti između bitnih aktera u zaštiti sistema od sajber napada. U većini zemalja nažalost dominira fragmentaran pristup (Maurer & Nelson, 2021).

Upravo zbog svih ograničenja za postizanje bolje sajber bezbednosti, možda je najvažnije podizanje svesti javnosti. Primenjujući sličan pristup kao i Aldasoro, Gambacora, Giudici & Leach (2020b), uporedila sam trend kretanja svesti javnosti o sajber incidentima u SAD, Ujedinjenom Kraljevstvu i u Srbiji (grafika 2). Može se primetiti da u SAD i Ujedinjenom Kraljevstvu svest javnosti kontinuirano raste, a naročito od 2017 godine, kada se desio globalni WannaCry sajber incident. U Srbiji se međutim povremeno povećava svest javnosti, izazvana događajima povezanim sa sajber napadima. Jedna zanimljiva uporedna analiza kampanja o podizanju svesti javnosti o sajber bezbednosti u Ujedinjenom kraljevstvu i zemljama Afrike, istakla je dva zaključka: (i) da kampanje vode računa o specifičnim kulturnim aspektima, jer kampanje

u Ujedinjenom Kraljevstvu koriste više individualistički pristup, a kampanje u Africi kolektivistički pristup; (ii) da postoji veliki broj kontinuiranih kampanja u Ujedinjenom Kraljevstvu dok u Africi postoji ograničen broj kampanja, moguće zbog nedostatka resursa (Bada, Sasse, & Nurse, 2015). U SAD nacionalna kampanja nosi naziv STANI.RAZMISLI.POVEŽI SE, a oktobar 2021. god. je proglašen mesecom svesti o sajber bezbednosti. Može se stoga zaključiti da postoji prostor i potreba za podizanjem svesti javnosti o sajber rizicima u našoj zemlji. Često se navodi da nije pitanje da li će se sistemski sajber napad desiti, nego kada će se desiti (Maurer & Nelson, 2021; Donas, 2021).

Grafika 2: Svest javnosti, Srbija, Ujedinjeno Kraljevstvo i SAD, juli 2010 – juli 2021

Izvor: Google Trends.

Napomene: Reči pretrage su „sajber napad“ za Srbiju i „sajber incident“ za Ujedinjeno kraljevstvo i SAD. Relevantni događaji u Srbiji: (1) decembar 2013, najava albanske sajber grupe Anonimusi da će izvršiti napade na veb stranice više srpskih javnih institucija; (2) maj 2017, globalni WannaCry sajber incident; (3) mart 2020, javno komunalno preduzeće Informatika je bilo meta uspešnog zlonamernog sajber incidenta; (4) decembar 2020, SAD optužuju Rusiju za seriju sajber napada; (5) maj 2021, Norveška je poklonila Srbiji platformu za simuliranje sajber napada.

Izgradnja nacionalnih kapaciteta za sajber bezbednost uključuje razvoj menadžerskih, tehničkih, socijalnih, pravnih, političkih i regulatornih inicijativa kako bi se povećala otpornost nacije na povrede sajber sigurnosti, na sajber kriminal i terorizam (Dutton, Creese, Shillair, & Bada, 2019). „Srbija ima dobar rezultat u mnogim oblastima kapaciteta za sajber bezbednost, dobro razume postojeće nedostatke i mogućnosti za izgradnju kapaciteta“, navodi se u izveštaju „Prve procene modela zrelosti kapaciteta za sajber bezbednost“ koji se tiče naše zemlje, a koji je sprovedla Svetska banka (World Bank Press Release, 2020). Izveštaj sugerise

vladi naše zemlje da se posveti inter alia izazovu zadržavanja stručnjaka iz oblasti sajber bezbednosti. U izgradnji efikasnog sistema zaštite od sajber napada, važno je imati dobro edukovan kadar. Potrebe rastu za zapošljavanje kadrova koji poseduju ne samo tehničko znanje, nego i netehničko znanje u oblasti izazova sa kojima se finansijski sistem suočava, kontinuiteta poslovanja ili ljudskih resursa (Maurer & Nelson, 2021; Donas, 2021; Uddin, Ali, & Hassan, 2020). Centralna banka Francuske, na primer, sarađuje sa školama u cilju formiranja raznoraznih vrsta kadrova neophodnih u oblasti sajber bezbednosti (Donas, 2021). Deo radnika otpuštenih tokom pandemije mogao bi takođe da se prekvalifikuje za tražena nova zanimanja.

Zaključak

U pojedinim infrastrukturnim oblastima od kritične važnosti, između ostalog i u bankarskom sektoru, sajber bezbednost postaje sve više pitanje nacionalne bezbednosti. Ovo zbog toga što negativne posledice zlonamernih sajber incidenata na finansijske institucije mogu biti sistemske prirode.

Obzirom na to da broj i sofisticiranost sajber napada konstantno raste, tako i sistem sajber bezbednosti treba konstantno da se unapređuje. U Srbiji, konkretno, ima prostora da se unapredi svest javnosti o sajber rizicima. Ako ostavimo po strani medije, pojedine institucije od javnog značaja mogu doprineti tom zadatku.

Srbija ima visoko kvalifikovanu radnu snagu, ali je problem što tradicionalno predstavlja zemlju koja je izvor migracije ljudi. Naročito je velik izazov za javne vlasti migratornih zemalja zadržavanje visoko obrazovanih kadrova. Buduća domaća naučna istraživanja i preporuke treba da budu fokusirana ne samo u zaustavljanje „odliva mozgova“ nego i stvaranje uslova za njihov povratak u zemlju..

Literatura

1. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020a). Operational and Cyber Risk in the Financial Sector. BIS Working Paper 840.
2. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020b). The Drivers of Cyber Risk. BIS Working Paper 865.
3. Bada, M., Sasse, A., & Nurse, J. (2015). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? Digital Economy. Conference Paper.
4. BIS. (2021). Covid-19 and cyber risk in the financial sector. BIS Bulletin 37.
5. BizLife. (2017). NBS žrtva prevare teške 175.500 evra. BizLife. Retrieved 04 04, 2021, from <https://www.bizlife.rs/nbs-zrtva-prevare-teske-175-500-evra/>
6. Brauchle, J.-P., Göbler, M., Seiler, J., & von Busekist, C. (2020). Cyber Mapping the Financial System. Carnegie Endowment for International Peace.
7. Brenner, J. (2017). Keeping America Safe: Toward More Secure Networks for Critical Sectors. Report on a Series of MIT workshops, MIT Internet Policy Research Initiative.
8. Britz, M. (2013). Computer Forensics and Cyber Crime. An Introduction (3 ed.). Pearson Education .
9. Canalys. (2021). Global cloud services market surges US\$10 billion in Q4 2020. Retrieved 03 10, 2020, from <https://www.canalys.com/newsroom/global-cloud-market-q4-2020>
10. CapGemini & EFMA. (2021). World Retail Banking Report 2021.
11. Carrière-Swallow, Y., & Haksar, V. (2021). Let's build a better data economy. IMF Finance & Development.
12. Casu, B., Ferrari, A., Girardone, C., & Wilson, J. (2016). Integration, Productivity and Technological Spillovers: Evidence for Eurozone Banking Industries. European Journal of Operational Research, 255(3), 971-983.
13. Cybersecurity & Infrastructure Security Agency. (2020, 06 23). Alert (AA20-106A). Guidance on the North Korean Cyber Threat. Retrieved from An official website of the United States government: <https://us-cert.cisa.gov/ncas/alerts/aa20-106a>
14. Danielsson, J., & Macrae, R. (2019). Systemic consequences of outsourcing to the cloud. VOX EU, CEPR policy portal.
15. Donas, C. (2021). Cybersecrurité, une armée d'experts de tous horizons. L'AGEFI Hebdo. Retrieved 05 12, 2021, from <https://www.agefi.fr/emploi/actualites/hebdo/20210506/cybersecrurite-armee-d-experts-tous-horizons-320305>
16. Dutton, W., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? Journal of Information Policy, 9, 280-306.
17. Ernst & Young. (2020). How COVID-19 could change the way we bank in Europe. Retrieved 03 22, 2021, from https://www.ey.com/en_gl/financial-services-emeia/how-covid-19-could-change-the-way-we-bank-in-europe
18. European Systemic Risk Board. (2020). Systemic Cyber Risk. European Systemic Risk Board. European System of Financial Supervision.
19. EUROPOL. (2020). Internet Organized Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.
20. Flinders, K. (2020). HSBC chooses AWS for public cloud business operations. ComputerWeekly.com. Retrieved 03 20, 2021, from <https://www.computerweekly.com/news/252486161/HSBC-chooses-AWS-for-public-cloud-business-operations>
21. G20 Communiqué. (2017). Communiqué G20 Finance Ministers and Central Bank Governors Meeting. (str. 1-5). Baden Baden, Germany: G20 Germany 2017.
22. G20 Financial Stability Board. (2018). Cyber Lexicon. Financial Stability Board.
23. G20 Financial Stability Board. (2020). Effective Practices for Cyber Incident Response and Recovery. Consultative Document. Financial Stability Board.

24. G20 Financial Stability Board. (2021). FSB Work Programme for 2021. Financial Stability Board.
25. Grant, E. (2021). The rise of biometric technology in banking. Finance Digest. Retrieved 03 21, 2021, from <https://www.financedigest.com/the-rise-of-biometric-technology-in-banking.html>
26. HSBC. (2020). Exploring the power of quantum computing. Retrieved 03 20, 2021, from <https://www.hsbc.com/news-and-media/hsbc-news/exploring-the-power-of-quantum-computing>
27. IMF Fintech Notes 20/01. (2020). Distributed Ledger Technology Experiments in Payments and Settlements. International Monetary Fund.
28. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. IMF Working Papers. WP/17/185.
29. Maurer, T., & Nelson, A. (2021). The global cyber threat. IMF Finance & Development.
30. S & P Global Market Intelligence. (2020). The world's 100 largest banks, 2020.
31. Tanjug. (2017). NBS: Nije bilo nikakvog „sajber napada“. Politika. Retrieved 04 04, 2021, from <http://www.politika.rs/sr/clanak/381317/Ekonomija/NBS-Nije-bilo-nikakvog-sajber-napada>
32. Thornton, P. (2020). Cyber attacks could cause financial crisis, says ECB chief Christine Lagarde. Independent (online). Retrieved 04 11, 2020, from <https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html>
33. Uddin, H., Ali, H., & Hassan, K. (2020). Cybersecurity Hazard and Financial System Vulnerability. A Synthesis of Literature. Risk Management, 22, 239–309.
34. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-Threat Perception and Risk Management in the Swedish Financial Sector. Computers & Security, 105, article id 102239.
35. Vavra, S. (2021, 04 12). Fed chair deems cyber threat top risk to financial sector. CyberScoop (online). Retrieved 04 30, 2020, from <https://www.cyberscoop.com/federal-reserve-chairman-jerome-powell-cyberattack/>
36. World Bank Press Release. (2020). Serbia Has Undertaken Critical Steps in Cybersecurity, Says First Cybersecurity Capacity Maturity Model Assessment. The World Bank.
37. Zec, S. (2021). Digitalizacija bankarskog sektora i uloga Udruženja banaka Srbije. Bankarstvo, 50(1), 6-9.

Received: 24.06.2021

Approved: 07.10.2021

DOI: 10.5937/bankarstvo2103140P

CYBER INCIDENTS CONNECTED TO FINANCIAL INSTITUTIONS

Ksenija Popović, PhD student,
Alpen Adria University in Austria
email: ksenijapo@edu.aau.at

Summary:

The main topic of the paper is the accelerated digital transformation of financial institutions, which, in addition to the advantages, also brings an increased risk of cyber incidents. Cyber incidents can cause systemic damage and, therefore, building a good cyber security system goes beyond individual financial institutions. Based on a comparative analysis of the trend of public awareness about cyber-attacks, the conclusion of this paper is that, unlike developed countries, public awareness in Serbia has no continuous but occasional growth caused by individual events related to cyber-attacks. Designing a national campaign to raise public awareness about cyber security, as well as training and retaining highly qualified personnel, are two recommendations that are self-imposed after the observation and analysis of information on cyber incidents in Serbia.

Keywords: Malicious cyber incident; digital transformation; financial institutions; cyber security

JEL classification: G20, K24

Introduction

In 2017, G20 warned that cyber incidents may endanger the stability of the financial sector (G20, 2017) and for that reason, assigned the task to its Financial Stability Board to stock-take national regulations and effective practices related to cyber incidents. Countries that are members of G20 account for 80% of the world's GDP and 60% of the world's population. In April 2020, the mentioned Financial Stability Board provided recommendations to financial institutions on what to do before, during, and after a cyber incident (G20 Financial Stability Board, 2020). Enhancing cyber resilience is also among the priority tasks in the Financial Stability Board's work program for 2021 (G20 Financial Stability Board, 2021).

In February 2020, Christine Lagarde, president of the European Central Bank, warned that a well-organized cyber incident on major financial institutions could cause a serious financial crisis (Thornton, 2020). At the same time, the European Systemic Risk Board, responsible for macroprudential oversight in the EU, published its report Systemic Cyber Risk. This report states that „...it is not inconceivable that in future, a large-scale cyber incident in the financial sector could create disruption on such a scale that it has the potential to have serious negative consequences for the internal market and the real economy“ (European Systemic Risk Board, 2020, p. 23). In April 2021, Federal Reserve Chairman, Jarome Powel, said that cyber risk connected to financial institutions is above and beyond any other risks to the economy (Vavra, 2021).

Through observation and analysis of already existing information, the aim of this paper is to answer two questions: first, why so much attention is focused on cyber incidents and second, what is the situation on the financial market of Serbia. The structure of the work is as follows. The first part lists the advantages and disadvantages of technological progress in financial institutions. The definition of a cyber incident, threat actors, types and specific examples of cyber incidents are given in the second part. The third part defines systemic cyber risk and analyzes measures to improve cyber security, including a couple of recommendations for Serbia.

Digital Transformation

Digital transformation encompasses small and large technological improvements that not only shift the offer of financial institutions towards online and digital services, but also include the application of modern technology in all spheres of work. During the process of recruiting new employees, for example, banks more often use artificial intelligence to short-list candidates based on keywords from their résumés. On the one side, digitalization makes internal processes more efficient, and on the other side, it changes communication channels towards customers. Nowadays almost all banks have their profiles on social networks (Facebook, Twitter, LinkedIn...), while bots communicate with clients on chat platforms thanks to artificial intelligence. Banks also offer digital account opening, instant payments within a few seconds, services in digital branches, electronic cash loans... E-banking enables customers to approach and use their accounts anytime and anywhere. M-banking enables banks to sell their products through applications for mobile phones.

According to empirical research, in the period from 1992 to 2014, the banking sectors of the Eurozone countries develop by converging towards the best available technology and the productivity of the banking sectors grows due to constant technological shifts, albeit at decreasing speed (Casu, Ferrari, Girardone, & Wilson, 2016). The banking sector of Serbia has kept pace with these technological

changes (Zec, 2021), mostly because it is dominated by developed foreign banks.

In the financial market, there are a small number of those who are leaders in technological development, on the one hand, and there is a majority who follow market leaders in an effort to reduce the technological gap, on the other hand. Here are a few examples of the advanced digital transformation carried out by the large bank groups: HSBC Group, the sixth, and Bank of America, the eighth largest banking group in the world according to total assets at the end of 2019 (S & P Global Market Intelligence, 2020):

- **Cloud computing** is a new technology that provides an internet place or cloud giving individuals and banks (as well as other companies) the opportunity to use resources, such as virtual machines, database, memory, services, storage, messaging, etc. Therefore, cloud computing contributes, among other things, to lower computer infrastructure costs, better reporting and analysis, faster and easier access to data, better insight into the potential of cross-selling. In October 2019, Bank of America ran 80% of its workload via an internal cloud, reducing the number of its servers from 200.000 to 70.000. Now Bank of America aims to move its workload to a public cloud (CapGemini & EFMA, 2021, p. 22). HSBC Bank announced in July 2020 that it has selected Amazon Web Services 'public cloud for its business operations globally (Flinders, 2020).

This internet place can be privately owned or public (in which case, it is hosted by another party, i.e., a cloud provider). The top 4 cloud providers are Amazon Web Services, Microsoft Azure, Google Cloud and Alibaba Cloud. According to the Canalys estimates (Canalys, 2021), their market participation as of Q4 2020 is dominant in comparison to other cloud providers (Figure 1). Although the data do not refer only to the banks' cloud services spending, it is clear that there is a trend to homogenize around several largest cloud vendors.

Figure 1: *Worldwide Cloud Infrastructure Services Spent USD 39.9 billion, Q4 2020*

Source: Canalys (Canalys, 2021)

- The HSBC bank participates also in the European NEASQC research project related to the application of **quantum computing technology**. NEASQC is an abbreviation for Next Application of Quantum Computing. It is believed that quantum computers have higher capabilities to tackle high complex tasks in comparison to today's computers (HSBC, 2020).

- **Biometric technology** in banking means that soon PIN codes and passwords will be replaced by human biological characteristics. HSBS bank announced the use of customer voice verification (Grant, 2021).

Even more advanced countries think about new technologies that can be a potential game-changer for how they will operate in the future:

- **Distributed ledger technology (DLT)** has been viewed as a potential platform for the third generation of payment systems, after the paper-based generation and the generation based on batch processing (IMF Fintech Notes 20/01, 2020). For example, the central bank of Canada and monetary authorities of Singapore bilaterally connected their experimental payment systems in which a central bank digital currency is used. They connected two different DLT platforms. Another example, SWIFT created a new GPI platform to improve the speed of payments. Although this platform is not a DLT platform, research is ongoing to enable blockchain companies to connect to the SWIFT GPI platform (IMF Fintech Notes 20/01, 2020). Blockchain is a type of DLT platform.

With the onset of the pandemic, financial institutions are trying to adapt to a volatile, uncertain and complex environment. The lockdowns that followed in all countries during the corona virus pandemic forced banks and other financial institutions to close their branches and customers to increasingly turn to online services. The portion of contactless payments, online payments and card payments increases, while the portion of payments in cash decreases (Ernst & Young, 2020). Due to the pandemic, a larger number of employees of financial institutions started working from home, which means that employees no longer work in the virtual and physical space under the control of those financial institutions. We are witnessing the acceleration of the implementation of digital technology.

However, such acceleration of digital transformation also has certain disadvantages. During the pandemic, the number of cyber-attacks on financial institutions increased so much that the financial sector became the second most common target of attacks, right after the health sector (BIS, 2021). The question is whether the financial sector can keep pace with the growing number of malicious cyber-attacks.

Cyber Incident

Cyber incidents are becoming more frequent, more innovative, more sophisticated, in multiple forms while cyber risk is only partially understood (Kopp, Kaffenberger, & Wilson, 2017). Every financial institution is exposed to cyber risk, because there is no perfect cyber security system - "some unknown system loopholes always exist irrespective of technological sophistication" (Uddin, Ali, & Hassan, 2020, p. 9). The idea of my work is to shed light on the

topic of cyber incidents, starting with the definition, the actors, and types of cyber incidents. According to the Cyber Lexicon (G20 Financial Stability Board, 2018, p. 9), cyber incident is: “a cyber event that:

- jeopardizes the cyber security of an information system or the information the system processes, stores or transmits; or
- violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.”

Cyber incidents can thus be accidental or malicious. But we are interested here primarily in malicious cyber incidents, because they are more numerous. For the sake of precision, the difference between a cyber-attack and a cyber incident is that the attack precedes the incident. Although, in Serbia, the term cyber-attack is used to describe both the attack and the incident.

There are several actors of cyber threats: national, criminal, terrorist, hacktivists or insiders, with different motives (see table 1). North Korea is often considered as a sponsor of cyber groups that are involved in financial theft, money laundering and extortion campaigns (Varga, Brynielsson, & Franke, 2021; Cybersecurity & Infrastructure Security Agency, 2020). Criminal cyber groups are still the most common threat actors, and some of the well-known are Carbanak, Silence, Lazarus, OldGremlin and Black Shadow.

Table 1:

Threat actor	Motivation
National	Geopolitical and ideological
Criminal	Enrichment
Terrorist groups, hacktivists	Ideological, discontent
Insider threats	Greed, disgruntlement

Source: ESRB (European Systemic Risk Board, 2020).

There are several types of cyber incidents, and the most common types with a brief description are listed in Table 2. However, there are several common characteristics of different types of cyber incidents. First, they are hard to detect. The research, which included financial institutions around the world in the period from 2002-2019, concluded that it takes an average of 251 days from the moment of occurrence to the moment of detecting losses caused by cyber incidents (Aldasoro, Gambacorta, Giudici, & Leach, 2020a). Second, due to their anonymity

and irreversibility of transactions, cryptocurrencies have become established as a method of paying cyber attackers by victims of attacks (EUROPOL, 2020). Third, financial institutions are not always willing to report cyber incidents due to reputational risk (Britz, 2013; Varga, Brynielsson, & Franke, 2021).

Table 2:

Type of cyber incident	Short description
Malware	Software designed to create damage(for example, computer viruses, Trojans...)
Man-in-the middle	Insertion in the middle of a two-party transaction
Cross-site scripting	Abuse of web application vulnerability that the victim, the user of the application otherwise trusts
Phishing	Imitating a trustworthy entity in a digital communication, to gain a victim's trust
Password cracking	Identification of an unknown password
A zero-day exploit	Abuse of discovered software or hardware vulnerability
Distributed Denial of Service(DDoS)	Multiple attack on a target(for example a server, website or network) that causes denial of service for the users

Source: BIS bulletin no. 37 (BIS, 2021) and Aldasoro, Gabacorta, Giudici & Leach (2020b).

At the official web page of Carnegie Endowment for International Peace, there is a database containing relevant cyber incidents connected with financial institutions from around the world (so called: Timeline of Cyber Incidents Involving Financial Institutions - Carnegie Endowment for International Peace). The Carnegie Endowment for International Peace is an international analytical think tank that was founded in 1910. Types of cyber incidents recorded in this database are data breach, theft, espionage, and disruption. Here are a few worldwide examples of cyber incidents:

- In January 2021, the central bank of New Zealand suffered a data breach.
- In December 2020, an Israeli insurance company was under attack of Black Shadow cybercriminal group, which demanded 200 bitcoin in exchange for stolen data.
- In September 2020, several Hungarian banks were disrupted due to the DDoS attack.
- In August 2020, a bank from Morocco suffered a breach of customer accounts and unauthorized execution of transactions.
- In March 2020, a criminal cyber group called OldGremlin entered networks of several Russian banks, encrypted data and demanded a ransom.

Based on publicly available records of the National CERT of the Republic of Serbia (CERT is an acronym for Computer Emergency Response Team), the most common cyber incidents connected to financial institutions in our country relate to malicious phishing campaigns aimed at bank clients (<https://cert.rs/obavestjenja.html#613>). Media reported in May 2017 that there was an attempt to cause material damage to the Institute for Manufacturing Banknotes and Coins, which operates within the National Bank of Serbia, through a malicious phishing message (Tanjug, 2017; BizLife, 2017).

In fact, all those sectors that are critical to a country's economy, such as oil pipelines, electricity supply, the banking sector, etc., should be subject to national security when it comes to cyber incidents (Aldasoro, Gambacorta, Giudici, & Leach, 2020b; Brenner, 2017).

Systemic Cyber Risk

There is a high level of interconnectedness across financial institutions, and particularly across their IT systems. This contributes to the higher speed and wider transmission of the negative consequences of a potential cyber incident. However not every cyber incident is of a systemic nature. The Carnegie Endowment for International Peace report proposes several specific conditions that should be cumulatively met to categorize a cyber incident into a systemic one (Brauchle, Göbler, Seiler, & von Busekist, 2020):

- focus on a systemically important financial institution or several financial institutions (functional channel);
- duration of the incident lasts 2 hours and/or is long enough to prevent end-of-day settlement;
- direct and indirect financial loss exceeds the level of the bank's capital (financial channel);
- loss of confidence measured by the duration of the news of the incident, the number of media involved and the geographical area they cover (confidence channel).

The European Systemic Risk Board analyzed several hypothetical systemic cyber risks (European Systemic Risk Board, 2020), among them: (i) payment system disruption of a domestic systemically important bank and (ii) wiping of the account balance data followed by unauthorized payments. In both cases, the longer cyber-attack lasts, the greater the negative consequences are. A general loss of confidence triggers the systemic character of a cyber incident. "For instance, if – in the aftermath of a successful malicious cyber incident – the customers of a bank were to find all account balances to be zero or unavailable for a prolonged period of time, and the institution were to be unable to resolve the situation within a reasonable time frame, it is conceivable that panic could start to spread. As a complicating factor, in such an instance fake news and disinformation may spread via social media, potentially as part of the incident, further destabilizing the markets and society." (European Systemic Risk Board, 2020, p. 38).

There is an opinion that the transfer of the IT function of financial institutions to the cloud can also be a source of systemic cyber risk (Danielsson & Macrae, 2019; Aldasoro, Gambacorta, Giudici, & Leach, 2020b). Given the trend of homogenization around the largest cloud vendors, any cyber or other incident on the cloud can affect multiple financial institutions at the same time. We remember the fire in March 2021, when out of four OVH cloud data centers in Strasbourg, one was destroyed and the other damaged. Millions of websites were out of order, including those from various government agencies, banks, newspapers, shops, etc. OVH cloud is the largest European cloud supplier. Danielsson and Macrae (2019) suggest regulating the operations of cloud providers, as the question is if a private cloud provider would give priority to customers from their own or another country, whether it would give priority to the government or financial institutions - in case of solving the consequences of a malicious cyber incident.

One of the important tasks for increasing the level of cyber security is the introduction of standards and regulations at the national and international level. Setting standards and regulations in the area of cyberspace is important because "an individual company does not fully internalize the harm to public trust in the entire system when its customers' data are breached, and may thus invest less in cyber security than what would be in the public interest. This concern has special resonance in the financial system, where maintaining public confidence is crucial" (Carrière-Swallow & Haksar, 2021, p. 13). Some central banks, such as the central bank of France, have special units (The Paris Resilience Group or le groupe de place Robustesse) dedicated to simulating various shock scenarios, from natural disasters to triggered crises such as a cyber-attack. The goal of these units is to maintain credibility in institutions and strengthen resilience in the event of major operational crises (Donas, 2021).

Since cyber-attacks occur beyond the concepts of physical borders between countries, because they take place in a virtual cyberspace, international cooperation and data exchange is very important. In November 2020, the Carnegie Endowment for International Peace and the World Economic Forum published an International Strategy to Better Protect the Global Financial System against Cyber Threats. In a large number of countries, including ours, CERT teams have been established with the aim of promptly responding to possible cyber incidents. Equally strategically important is the precise distribution of responsibilities within the country, as well as the demarcation of national jurisdictions in the event of a cyber-attack. Only a few countries in the world have a clear division of roles and responsibilities between important actors in protecting the system from cyber-attacks. Unfortunately, a fragmented approach dominates in most countries (Maurer & Nelson, 2021).

Precisely because of all the limitations for achieving better cyber security, perhaps the most important thing is to raise public awareness. Applying a similar approach to Aldasoro, Gambacorta, Giudici & Leach (2020b), I compared the trend of public awareness of cyber incidents in the USA, the United Kingdom and Serbia (Figure 2). It can be noticed that in the USA and the United Kingdom, public awareness is continuously growing, especially since 2017, when the

global WannaCry cyber incident took place. In Serbia, however, public awareness is occasionally increasing, caused by events related to cyber-attacks. An interesting comparative analysis of cybersecurity awareness campaigns in the UK and Africa highlighted two conclusions: (i) that campaigns take into account specific cultural aspects, as campaigns in the UK use a more individualistic approach and campaigns in Africa a collectivist approach; (ii) that there are a large number of ongoing campaigns in the United Kingdom while in Africa there are a limited number of campaigns, possibly due to lack of resources (Bada, Sasse, & Nurse, 2015). In the United States, the national campaign is called STOP. THINK. CONNECT, and October 2021 has been declared the month of cyber security awareness. It can therefore be concluded that there is room and need to raise public awareness about cyber risks in our country. It is often stated that the question is not whether a systemic cyber-attack will happen but when it will happen (Maurer & Nelson, 2021; Donas, 2021).

Figure 2: Public Awareness, Serbia, the United Kingdom and the USA, July 2010 - July 2021

Source: Google Trends.

Notes: Search words are "cyber-attack" for Serbia and "cyber incident" for the United Kingdom and the USA. Relevant events in Serbia: (1) December 2013, the announcement of the Albanian cyber group Anonymous that they would carry out attacks on the websites of several Serbian public institutions; (2) May 2017, the global WannaCry cyber incident; (3) March 2020, the public utility company Informatika was the target of a successful malicious cyber incident; (4) December 2020, the United States accuses Russia of a series of cyber-attacks; (5) May 2021, Norway donated to Serbia a platform for simulating cyber-attacks.

National cybersecurity capacity building involves the development of managerial, technical, social, legal, policy, and regulatory initiatives to enhance the resilience of a nation to cybersecurity breaches, cybercrime, and terrorism (Dutton, Creese, Shillair, & Bada, 2019). "Serbia

performs well across many areas of cybersecurity capacity and has a strong understanding of existing gaps and opportunities for capacity building”, according to a report of the First Cybersecurity Capacity Maturity Model Assessment concerning our country, and conducted by the World Bank (World Bank Press Release, 2020). The report suggests to the government of our country to focus, inter alia, on the challenge of retaining experts in the field of cyber security. In building an effective system of protection against cyber-attacks, it is important to have a well-educated workforce. The needs are growing for the employment of workforce not only with technical knowledge, but also non-technical knowledge in the field of challenges financial system face, business continuity or human resources (Maurer & Nelson, 2021; Donas, 2021; Uddin, Ali, & Hassan, 2020). The central bank of France, for example, cooperates with schools to train the various types of workforce needed in the field of cyber security (Donas, 2021). Some of the workers laid off during the pandemic could be also retrained for the required new occupations.

Conclusion

In certain critical infrastructure areas, including the banking sector, cyber security is increasingly becoming a national security issue. This is because the negative consequences of malicious cyber incidents on financial institutions can be systemic in nature.

Given that the number and sophistication of cyber-attacks is constantly growing, the cyber security system needs to be constantly improved as well. In Serbia, in particular, there is room to improve public awareness of cyber risks. Leaving aside the media, certain institutions of public importance can contribute to this task.

Serbia has a highly qualified workforce, but the problem is that it traditionally represents a country that is a source of human migration. Retaining highly educated staff is a particular challenge for the public authorities of migrant countries. Future domestic scientific research and recommendations should be focused not only on stopping the “brain drain” but also on creating conditions for their return to the country.

References

1. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020a). Operational and Cyber Risk in the Financial Sector. BIS Working Paper 840.
2. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020b). The Drivers of Cyber Risk. BIS Working Paper 865.
3. Bada, M., Sasse, A., & Nurse, J. (2015). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? Digital Economy. Conference Paper.
4. BIS. (2021). Covid-19 and cyber risk in the financial sector. BIS Bulletin 37.
5. BizLife. (2017). NBS žrtva prevare teške 175.500 evra. BizLife. Retrieved 04 04, 2021, from <https://www.bizlife.rs/nbs-zrtva-prevare-teske-175-500-evra/>
6. Brauchle, J.-P., Göbler, M., Seiler, J., & von Busekist, C. (2020). Cyber Mapping the Financial System. Carnegie Endowment for International Peace.
7. Brenner, J. (2017). Keeping America Safe: Toward More Secure Networks for Critical Sectors. Report on a Series of MIT workshops, MIT Internet Policy Research Initiative.
8. Britz, M. (2013). Computer Forensics and Cyber Crime. An Introduction (3 ed.). Pearson Education .
9. Canalys. (2021). Global cloud services market surges US\$10 billion in Q4 2020. Retrieved 03 10, 2020, from <https://www.canalys.com/newsroom/global-cloud-market-q4-2020>
10. CapGemini & EFMA. (2021). World Retail Banking Report 2021.
11. Carrière-Swallow, Y., & Haksar, V. (2021). Let's build a better data economy. IMF Finance & Development.
12. Casu, B., Ferrari, A., Girardone, C., & Wilson, J. (2016). Integration, Productivity and Technological Spillovers: Evidence for Eurozone Banking Industries. European Journal of Operational Research, 255(3), 971-983.
13. Cybersecurity & Infrastructure Security Agency. (2020, 06 23). Alert (AA20-106A). Guidance on the North Korean Cyber Threat. Retrieved from An official website of the United States government: <https://us-cert.cisa.gov/ncas/alerts/aa20-106a>
14. Danielsson, J., & Macrae, R. (2019). Systemic consequences of outsourcing to the cloud. VOX EU, CEPR policy portal.
15. Donas, C. (2021). Cybersecrîté, une armée d'experts de tous horizons. L'AGEFI Hebdo. Retrieved 05 12, 2021, from <https://www.agefi.fr/emploi/actualites/hebdo/20210506/cybersecrîte-armee-d-experts-tous-horizons-320305>
16. Dutton, W., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? Journal of Information Policy, 9, 280-306.
17. Ernst & Young. (2020). How COVID-19 could change the way we bank in Europe. Retrieved 03 22, 2021, from https://www.ey.com/en_gl/financial-services-emeia/how-covid-19-could-change-the-way-we-bank-in-europe
18. European Systemic Risk Board. (2020). Systemic Cyber Risk. European Systemic Risk Board. European System of Financial Supervision.
19. EUROPOL. (2020). Internet Organized Crime Threat Assessment (IOCTA). European Union Agency for Law Enforcement Cooperation.
20. Flinders, K. (2020). HSBC chooses AWS for public cloud business operations. ComputerWeekly.com. Retrieved 03 20, 2021, from <https://www.computerweekly.com/news/252486161/HSBC-chooses-AWS-for-public-cloud-business-operations>
21. G20 Communiqué. (2017). Communiqué G20 Finance Ministers and Central Bank Governors Meeting. (str. 1-5). Baden Baden, Germany: G20 Germany 2017.
22. G20 Financial Stability Board. (2018). Cyber Lexicon. Financial Stability Board.
23. G20 Financial Stability Board. (2020). Effective Practices for Cyber Incident Response and Recovery. Consultative Document. Financial Stability Board.

24. G20 Financial Stability Board. (2021). FSB Work Programme for 2021. Financial Stability Board.
25. Grant, E. (2021). The rise of biometric technology in banking. Finance Digest. Retrieved 03 21, 2021, from <https://www.financedigest.com/the-rise-of-biometric-technology-in-banking.html>
26. HSBC. (2020). Exploring the power of quantum computing. Retrieved 03 20, 2021, from <https://www.hsbc.com/news-and-media/hsbc-news/exploring-the-power-of-quantum-computing>
27. IMF Fintech Notes 20/01. (2020). Distributed Ledger Technology Experiments in Payments and Settlements. International Monetary Fund.
28. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber Risk, Market Failures, and Financial Stability. IMF Working Papers. WP/17/185.
29. Maurer, T., & Nelson, A. (2021). The global cyber threat. IMF Finance & Development.
30. S & P Global Market Intelligence. (2020). The world's 100 largest banks, 2020.
31. Tanjug. (2017). NBS: Nije bilo nikakvog „sajber napada“. Politika. Retrieved 04 04, 2021, from <http://www.politika.rs/sr/clanak/381317/Ekonomija/NBS-Nije-bilo-nikakvog-sajber-napada>
32. Thornton, P. (2020). Cyber attacks could cause financial crisis, says ECB chief Christine Lagarde. Independent (online). Retrieved 04 11, 2020, from <https://www.independent.co.uk/news/business/news/cyber-attack-financial-crisis-christine-lagarde-ecb-a9322556.html>
33. Uddin, H., Ali, H., & Hassan, K. (2020). Cybersecurity Hazard and Financial System Vulnerability. A Synthesis of Literature. Risk Management, 22, 239–309.
34. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-Threat Perception and Risk Management in the Swedish Financial Sector. Computers & Security, 105, article id 102239.
35. Vavra, S. (2021, 04 12). Fed chair deems cyber threat top risk to financial sector. CyberScoop (online). Retrieved 04 30, 2020, from <https://www.cyberscoop.com/federal-reserve-chairman-jerome-powell-cyberattack/>
36. World Bank Press Release. (2020). Serbia Has Undertaken Critical Steps in Cybersecurity, Says First Cybersecurity Capacity Maturity Model Assessment. The World Bank.
37. Zec, S. (2021). Digitalizacija bankarskog sektora i uloga Udruženja banaka Srbije. Bankarstvo, 50(1), 6-9.