Bankarstvo, 2017, vol. 46, br. 4
Primljen: 17.11.2017. Prihvaćen: 13.12.2017.

pregledni naučni članak

doi: 10.5937/bankarstvo1704134S

Darko Šehović

Udruženje banaka Srbije
darko.sehovic@ubs-asb.com

SAJBER OTPORNOST FINANSIJSKIH INSTITUCIJA

Prevod obezbedio autor

Rezime

Digitalizacija kao trend rezultat je već uveliko zahuktale četvrte industrijske revolucije i promena koje ona sa sa sobom nosi. Digitalizacija u svet finansijskih institucija uvodi mnoštvo novih elemenata kao što su novi kanali komunikacije i prodaje, nove količine podataka o klijentima i nove platforme za pružanje usluga. Trend digitalizacije prati i dominantna upotreba sajber prostora kao jednog od osnovnih kanala komunikacije, što u svet finansijskih institucija donosi i sve one stare i neke nove rizike koji prate sajber okruženje. Kako se finansijske institucije nose sa izazovima sa kojima se susreću, šta kaže domaća, a šta evropska regulativa i incijative po pitanju otpornosti finansijskih institucija na sajber rizike?

Ključne reči: sajber otpornost, sajber bezbednost, informaciona bezbednost, finansijske institucije, digitalizacija

JEL: K24, M15

Bankarstvo, 2017, Vol. 46, Issue 4
Received: 17.11.2017 Accepted: 13.12.2017

doi: 10.5937/bankarstvo1704134S

scientific review article

CYBER RESILIENCE OF FINANCIAL INSTITUTIONS

Darko Šehović

Association of Serbian Banks
darko.sehovic@ubs-asb.com

Translation provided by the author

Summary

Digitalization is the result of the fourth industrial revolution, which has been in full swing for some time, and the changes it brings about. In the world of financial institutions, digitalization introduces a host of new elements, such as new channels of communication and sales, new amounts of customer data, and new service platforms. The trend of digitalization has been accompanied by the dominant use of cyber space as one of the basic channels of communication, which burdens the world of financial institutions with both old and some new risks accompanying cyber environment. How do financial institutions cope with the emerging challenges, how do domestic and European regulations and initiatives respond when it comes to the resilience of financial institutions to cyber risks?

Keywords: Cyber resilience, cyber security, information security, financial institutions, digitalization

JEL: K24, M15

Ubrzan tehnološki razvoj, ekspanzija pametnih uređaja, omasovljavanje mobilnih uređaja kao neki od elemenata četvrte industrijske revolucije stavili su pred finansijske institucije izazove na koje su one odgovorile digitalizacijom, stvaranjem novih komunikacijskih kanala ka klijentima, kao i mnoštvom drugih inovativnih servisa. Roboti već uveliko pomažu u obradi informacija u unutrašnjim bankarskim sistemima, a sa sve većom tendencijom da posao obavljaju i u delu direktne komunikacije sa klijentom. Pored mnoštva servisa koji omogućavaju uspostavljanje komunikacije sa bankom sa bilo kog mesta i u bilo koje vreme i mnoštva zadovoljnih korisnika kao i prodavaca najrazličitijih tehnoloških rešenja, ove promene su donele i nove rizike o kojima će se tek raspravljati i čije posledice ćemo sagledavati u budućnosti.

Trenutni pejzaž sajber scene preplavljen je izveštajima o upadima u različite sisteme svetski poznatih kompanija i kompromitovanjem nebrojeno mnogo podataka o ličnosti. Upravo ovih dana saznajemo da je velika kompanija Yahoo u napadu koji se desio 2013. godine doživela proboj sistema u kome je kompromitovano ne kako se ranije tvrdilo milijardu podataka o klijentima već, kako stvari sada izgledaju, broj kompromitovanih podataka iznosi tri milijarde, što je u tom trenutku predstavljalo čitavu bazu podataka ove kompanije. Jedan od četiri najveća kreditna biroa u Sjedinjenim Američkim Državama doživeo je proboj i kompromitaciju 145 miliona podataka o građanima SAD, Velike Britanije i Kanade. Maliciozni softveri koji enkriptuju podatke korisnika i za uslugu povraćaja podataka traže otkupninu u bitkon kriptovaluti (tzv. kriptolokeri ili ransomware) poslednjih godina su sve prisutniji na internetu, a svoju veliku svetsku predstavu imali su u maju ove godine u operaciji WannaCry, koja je u roku od 15 sati uspela da napravi pravu pometnju na internetu i gobalnu pandemiju sa epiologom od preko 300.000 zaraženih računara u 150 zemalja sveta, od kojih je značajan procenat pripadao računarima po medicinskim ustanovama, što je dodatno zabrinulo javnost. Sve veći broj pametnih uređaja povezanih sa internetom (Internet of Things), čiji se broj procenjuje trenutno na četiri milijarde uređaja, a sa najavama da bi njihov broj mogao da dosegne i čitavih 20 milijardi do 2020. godine, uspeo je da pokaže i svoje drugo lice u napadu koji se odigrao krajem 2016. godine, a u kome je nekoliko miliona ovih uređaja napalo neke od najvećih provajdera internet usluga širom Amerike i u par sati učinilo nedostupnim neke od najvećih svetskih kompanija, time ponovo otvarajući debatu o nedovoljnoj uređenosti i podrazumevanoj bezbednosti ovakvih uređaja.

Ako ovom spisku dodamo i izveštaje o ukupnom gubitku od milijardu dolara koliko su štete izazvali Carbanak napadi na stotinak banka širom sveta u vremenskom intervalu od dve godine, kao i izveštaje o uspešno izvršenom napadu na Centralnu banku Bangladeša, u kome su napadači kompromitovali informacioni sistem banke i uspešno transferovali 951 milion dolara (81 milion nepovratno) ka različitim računima korišćenjem SWIFT mreže, kao i mnoštvo drugih kompromitacija informacionih sistema finansijskih institucija dobijamo stanje koje zahteva hitnu reakciju i odgovor.

Šta su posledice ovako razornih i u korenu veoma sofisticiranih napada?

Odgovor leži u već prisutnom trendu naprednih upornih pretnji (Advanced Persistant Threat ili APT) što po definiciji koju nam daje NIST predstavlja napadača sa visokim nivoom sofisticiranosti, značajnim resursima i tendencijom korišćenjem višesturukih vektora za napad koji u dužem vremenskom periodu u više navrata pokušava da ostvari cilj uspostavljanja dugotrajnog neprimećenog prisustva u mreži koju napada, a u cilju neovlašćenog pristupa informacijama. Uz ove podatke činjenica da su se u poslednjih nekoliko godina desili i veliki proboji informacionih sistema nekih državnih bezbednosnih agencija, što je za posledicu imalo javno objavljivanje i distribuiranje njihovih sajber „alata“, kao i sumnja u umešanost drugih država u ove događaje, baca novu svetlost na skorašnje incidente. Trend korišćenja visokosofisticiranih alata i sve češće uplitanje državnih agencija posebno zabrinjava i povećava nivo potencijalnog uticaja rizika po finansijske institucije. Posebno je poražavajuć podatak o prosečnom broju dana koji napadači

The accelerated technological development, the expansion of smart devices, the deployment of mobile devices are just some of the elements of the fourth industrial revolution that forced financial institutions to respond to the challenges by means of digitalization, creation of new communication channels for their clients, along with many other innovative services. Robots have already been helping in processing information in the internal banking systems, with the increasing tendency to perform the business operations concerning direct communication with the clients. In addition to the many services that enable the establishment of communication with the bank from any place and at any time to a lot of satisfied users and sellers of various technological solutions, these changes have incurred new risks that remain to be discussed and whose consequences will be considered in the future.

The current cyber landscape is flooded with reports of breaches into the various systems of the world-renowned companies, compromising the huge amounts of personal data. Only recently have we found out that in the 2013 attack the big Yahoo Company was the subject of a system breach, when the compromised data amounted to, not as previously claimed one billion pieces, but as it appears now, a total of three billion pieces, which at that time represented the complete database of this company. One of the four largest credit bureaus in the United States experienced a system breach when 145 million data about the citizens of the United States, Great Britain and Canada were compromised. Malicious software that encodes user data and requires ransom in bitcoins for the data retrieval (the so-called cryptocurrency or ransomware) has been increasingly present on the internet in recent years. In May this year, such software packages had their big world show in the WannaCry operation, when within 15 hours they managed to cause a major blip on the internet and a global pandemic with an epilogue of over 300,000 infected computers in 150 countries worldwide, a significant percentage of which were the computers in medical institutions, which additionally alarmed the public. A growing number of smart devices connected to the internet (Internet of Things), currently estimated at four billion, with some announcements that their number could reach up to 20 billion by 2020, also showed their true face in the attack that took place in late 2016. At that time, several million of these devices attacked some of the largest internet service providers across America and in a few hours made some of the world's largest companies inaccessible, thereby re-opening the debate about the insufficient regulation and the underlying security of such devices. Once we add to this list the reports of a total loss of one billion dollars as the damage caused by Carbanak attacks of hundreds of banks around the globe over a two-year period, as well as the reports of a successful attack on the Central Bank of Bangladesh, in which the attackers compromised the bank's information system and successfully transferred $ 951 million (81 million non-refundable) to different accounts using the SWIFT network, as well as many other cases of compromised information systems in financial institutions, it is evident that we are dealing with a situation that requires an urgent reaction and response.

What are the consequences of these disastrous and essentially very sophisticated attacks?

The answer lies in the already existing trend of Advanced Persistent Threats (APTs), which, according to the NIST definition, refers to attackers with a high level of sophistication, significant resources and tendency of using multi-handed attack vectors, who over a long period of time on several occasions try to establish a long-term unnoticed presence in the attacked network, with the aim of achieving unauthorized access to information. Furthermore, the fact that in the last few years there have been major intrusions into the information systems of some state security agencies, which resulted in the public announcement and distribution of their cyber "tools", along with the suspicion about the involvement of other states in these events, throws a new light on recent incidents. The trend of using highly-sophisticated tools in combination with the increasingly frequent interference of state agencies is particularly

provedu u različitim informacionim sistemima pre nego što budu uočeni i eliminisani iz njih, a što po izveštajima koje dobijamo danas iznosi oko 140 dana. Ova brojka jasno ukazuje na neadekvatnu pripremljenost postojećih sistema na ovakve pojave. Sama činjenica da je najčešći motiv današnjih napada finasijska zarada, stavlja finansijske institucije među prve na listi napadanih institucija u svetu a njihove rukovodioce pred izazove koje taj trend donosi.

Kako se Evropska unija pripremala i kako se priprema za oblast sajber bezbednosti možemo sagledati kroz analizu nekoliko ključnih dokumenta koji uređuju ovu oblast. Jedan od prvih dokumenata na ovu temu bila je strategija sajber bezbednosti objavljena 2013. godine. Ona je javnosti predstavila viziju Evropske komisije o načinima prevencije i odgovora na sajber bezbednosne izazove. Strategija sajber bezbednosti EU definiše sledeće principe sajber bezbednosti:

1. Osnovne vrednosti primenjuju se u digitalnom kao i u fizičkom svetu
2. Zaštita osnovnih prava, sloboda izražavanja, ličnih podataka i privatnosti
3. Pristup za sve
4. Demokratsko i efikasno upravljanje
5. Deljena odgovornost u cilju bezbednosti

Pored definisanja osnovnih principa strategija definiše strateške prioritete i akcije:

1. Dostizanje sajber otornosti
2. Drastično smanjenje sajber kriminala
3. Razvoj politika sajber odbrane i kapaciteta u skladu sa Politikama bezbednosti i odbrane
4. Razvoj industrijskih i tehnloških resursa za potrebe sajber bezbednosti
5. Uspostavljanje koherentne internacionalne sajber politike na nivou EU i promovisanje osnovnih vrednosti

Ovom Strategijom EU je pokušala da uspostavi putokaz za sve njene članove sa ciljem uspostavljanja bezbednog i pouzdanog sajber okruženja kao jednog od preduslova za uspešno funkcionisanje jedinstvenog digitalnog tržišta.

Dokument koji se detaljnije upušta u problematiku bezbednosti informacija i informacionih sistema je, u junu 2016. godine, usvojena Direktiva o bezbednosti mreža i informacionih sistema (NIS Directive EU 2016-1148), a čije puna primena se očekuje do maja 2018. godine. Ova direktiva kao jedan od glavnih motiva ima uspostavljanje sajber otpornosti u informacionim sistemima širom Evropske unije. Neki od ključnih delova ove direktive su:

1. Obaveza donošenja nacionalnih strategija u oblasti bezbednosti mreža i informacionih sistema
2. Kreriranje grupe za stratešku kooperaciju država članica
3. Kreiranje lokalnih timova za odgovor na računarske bezbednosne incidente (CSIRT), kao i nacionalnog tima, a u cilju postizanja operativne saradnje između država članica
4. Identifikaciju operatora kritičnih servisa
5. Uspostavljanje bezbednosnih zahteva i obaveze izveštavanja za operatore kritičnih servisa i za provajdere digitalnih usluga

Kreiranjem mreže CSIRTova širom Evrope učesnicima je omogućena brza razmena informacija, kreiranje baze znanja i prva pomoć u slučaju incidenata. Kao centralno telo za mrežu ovih timova izabrana je 2004. godine formirana Evropska agencija za mrežnu i informacionu sigurnost ENISA.

Grupa G7, koju sačinjavaju Kanada, Francuska, Nemačka, Italija, Japan, Ujedinjeno Kraljevstvo i EU, napravila je ekspertsku grupu, koja je sagledavajući rizike po finansijske institucije uočene u zemljama članicama definisala osnovne elemente sajber bezbednosti za finansijski sektor i objavila ih na sajtu Evropske komisije u oktobru 2016. godine. Ovaj dokument definiše osam elemenata na osnovu kojih finansijske organizacije mogu razvijati, usklađivati i ocenjivati svoje strategije i pravila funkcionisanja (okvir). Elementi koje ovaj dokument navodi kao osnovne za finansijske institucije su:

1. Uspostavljanje sajber strategije i okvira u skladu sa specifičnim sajber rizicima organizacije i u skladu sa internacionalnim, lokalnim i sektorski specifičnim standardima i uputstvima.
2. Uspostavljanje adekvatnog upravljanja u okviru organizacije zarad ostvarivanja ciljeva zadatih u strategiji i okviru.
3. Upravljanje sajber rizicima i kontrolama za prevenciju identifikovanih rizika.
4. Uspostavljanje sistemskog monitoringa u cilju brze detekcije sajber incidenata i procene efektivnosti uspostavljenih kontrola.

worrying and increases the level of potential risk impacts on financial institutions. Particularly devastating is the average number of days that attackers spend in various information systems before they are spotted and eliminated from them, which is, according to the reports we receive today, about 140 days. This figure clearly indicates the inadequate preparedness of the existing systems to these occurrences. The very fact that the most common motive of today's attacks is financial gain puts financial institutions among the first on the list of attacked institutions worldwide, forcing their leaders to face the challenges that this trend brings.

How did the European Union use to prepare itself and how is it preparing itself in terms of cyber security now can be seen from the analysis of several key documents governing this field. One of the first documents on this topic was the cyber security strategy published in 2013. It presented the European Commission's vision of ways to prevent and respond to cyber security challenges. The EU Cyber Security Strategy defines the following principles of cyber security:

1. Basic values are applied in digital as well as in the physical world
2. Protection of fundamental rights, freedom of expression, personal data and privacy
3. Access for all
4. Democratic and efficient management
5. Shared responsibility for security

In addition to defining the basic principles of strategy, it defines strategic priorities and actions:

1. The achievement of cyber resistance
2. A drastic reduction in cyber crime
3. Development of cyber defense policy and capacity in accordance with the Security and Defense Policy
4. Developing industrial and technological resources for cyber security
5. Establishing a coherent international cyber policy at the EU level and promoting core values

With this strategy, the EU has tried to establish a roadmap for all its members in order to establish a safe and reliable cyber environment as one of the prerequisites for the successful functioning of a single digital market.

The Network and Information Security Directive (NIS Directive EU 2016-1148) is a document that goes into more detail when it comes to information security and information systems, adopted in June 2016, and its full implementation is expected by May 2018. One of the main motives of this directive is the establishment of cyber resistance in information systems across the European Union. Some of the key parts of this directive are:

1. The obligation to adopt national strategies in the field of network security and information systems
2. The grouping for the strategic cooperation of the member states
3. Creating local teams to respond to computer security incidents (CSIRT), as well as the national team, in order to achieve operational cooperation between member states
4. Identification of critical service operators
5. Setting up security and reporting requirements for critical service operators and for digital service providers

The creation of the CSIRT network across Europe enables the participants to exchange information quickly, create a knowledge base and receive first aid in case of incidents. The European Union Agency for Network and Information Security (ENISA) was established in 2004 as the central body in charge of the network of these teams.

Group G7, comprised of Canada, France, Germany, Italy, Japan, the United Kingdom and the EU, formed an expert group which examined the risks for financial institutions detected in the member countries, defined the basic elements of cyber security for the financial sector and posted them on the European Commission's website in October 2016. This document defines the eight elements on the basis of which financial organizations can develop, align and evaluate their strategies and rules of functioning (frameworks). The elements that this document lists as basic for financial institutions are:

1. Establishing cyber strategies and frameworks in accordance with the specific cyber risks of the organization and in accordance with international, local and sector specific standards and guidelines.
2. Establishing adequate management within the organization in order to achieve the objectives set in the strategy and timeframe.

5. Uspostavljanje procesa procene odgovora na sajber incidente.
6. Uspostavljanje procesa oporavka svih vitalnih operacija nakon incidenta.
7. Uspostavljanje razmene informacija u cilju adekvatnog informisanja relevantnih učesnika sa pravovremenim i upotrebljivim informacijama o saber incidentima.
8. Kontinuirano učenje u cilju usklađivanja sajber strategije i okvira sa aktuelnim promenama u poslovanju i okruženju finansijskih organizacija.

Prepoznajući sajber rizike kao jedan od glavnih prioriteta za postizanje sigurnog i efikasnog funkcionisanja finansijskih tržišta, ova ekspertska grupa pokušala je da ukaže na osnovne elemente sajber bezbednosti, a zarad postizanja finansijske stabilnosti i očuvanja ekonomskog rasta tržišta. Ministri finansija i guverneri centralnih banka iz zemalja G7 dali su nedvomislenu podršku ovoj grupi i ideji da se definišu jasne smernice u oblasti sajber bezbednosti za čitavo finansijsko tržište.

Za specifične potrebe finansijskih institucija Odbor za platne sisteme Banke za međunarodna poravnanja (CPMI) i Međunarodna organizacija komisija za hartije od vrednosti (IOSCO) u junu 2016. godine objavili su Uputstvo za postizanje sajber otpornosti finansijskih institucija. Ovo uputstvo predstavlja dopunu osnovnih principa za finansijske institucije (PFMI) a u cilju postizanja sajber otpornosti. Principi koji se uzimaju kao osnov za ovo uputstvo su:

- Princip 2: Upravljanje
- Princip 3: Okvir za sveobuhvatno upravljanje rizicima
- Princip 8: Konačnost poravnanja
- Princip 17: Operativni rizik
- Princip 20: FMI links

Banka za međunarodna poravnanja uočavajući sve odlike današnjih sajber napada u ovom uputstvu definiše smernice za postizanje sajber otpornosti kroz sledeće korake (videti sliku 3.):

- Upravljanje
- Identifikacija
- Zaštita
- Detekcija
- Odgovor i oporavak
- Testiranje
- Situational awareness
- Učenje i evolucija

Imajući u vidu obavezu finansijskih institucija da u roku od dva sata uspostave svoje operacije (2hRTO) uputstvo daje dobro strukturirane smernice za redizajn u cilju postizanja adekvatne sajber otpornosti.

Neki od dokumenata koji nisu obavezujući, ali su svakako vredni pomena u ovom kontekstu su:

- NIST Cybersecurity framework verzija 1.0 (uz napomenu da je u pripremi nova unapređena verzija ovog dokumenta)
- Critical Security Controls verzija 6.0 Centra za internet bezbednost
- NIST 800-53 verzija 4

Ovi dokumenti su uveliko sazreli i dokazani u praksi i za razliku od međunarodnih standarda predmet su čestih usklađivanja sa aktuelnim trendovima tako da na efikasan način mogu pomoći u uspostavljanju merljivog sistema sajber otpornosti, implementaciju adekvatnih bezbednosnih mera i postizanja željenog nivoa bezbednosti. Pored svih u tekstu navedenih, banke su izložene i mnogim drugim standardima i smernicama poput PCI-DSS standarda ili novih uputstva koje kompanija SWIFT nakon spomenutih incidenta širom planete nameće svim učesnicima u sistemu (SWIFT Customer Security Programme), a koje imaju kao i u tekstu navedeni zakoni jasan cilj podizanje nivoa sajber otpornosti za sve učesnike u određenom sistemu.

Stanje u Republici Srbiji

Pregled zakonske regulative u Republici Srbiji u kontekstu informacione bezbednosti i finansijskih institucija izvršićemo u skladu sa datumima i redosledom donošenja propisa iz ove oblasti. Vlada Republike Srbije je 2010. godine donela Strategiju razvoja informacionog društva u RS do 2020. godine. U njoj je kao jedan od prioriteta definisala i informacionu bezbednost. Ova strategija dovela je do početka unapređenja pravnog i institucionalnog okvira za informacionu bezbednost u RS.

Sledeći po finansijske institucije bitan dokument objavila je Narodna banka Srbije u martu 2013. godine, a to je Odluka o minimalnim standardima za upravljanje informacionim sistemima finansijskih institucija (Službeni glasnik RS, br. 23/13, 113/13 i 2/17). Njome

3. Managing cyber risks and controls for the prevention of identified risks.
4. Establishing systemic monitoring in order to quickly detect cyber incidents and assess the effectiveness of established controls.
5. Establishing the process of assessment of the response to cyber incidents.
6. Establishing the process of recovery of all vital operations after an incident.
7. Establishing information exchange for the purpose of adequately informing relevant stakeholders based on the timely and usable information on cyber incidents.
8. Continuous learning in order to harmonize the cyber strategy and the frame with the current changes in the financial organizations' business and environment.

Having recognized cyber risks as one of the main priorities for achieving the safe and efficient functioning of financial markets, this expert group tried to point out the basic elements of cyber security, in order to achieve financial stability and preserve economic growth of the market. Finance ministers and central bank governors from the G7 countries unequivocally supported this group and the idea of defining the clear cyber security guidelines for the entire financial market.

For the specific needs of financial markets, in June 2016, the BIS Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) published the Guidance on Cyber Resilience for Financial Market Infrastructures. This document is a supplement to the basic principles for financial market institutions (PFMI) with a view to achieving cyber resistance. The principles that are taken as the basis for this document are:

- Principle 2: Management
- Principle 3: A framework for comprehensive risk management
- Principle 8: Finishing alignment
- Principle 17: Operational risk
- Principle 20: FMI links

The Bank for International Settlements, noting all the features of today's cyber attacks, in this document defines the guidelines for achieving cyber resistance through the following steps (see Figure 3):

- Management
- Identification
- Protection
- Detection
- Response and recovery
- Testing
- Situational awareness
- Learning and evolution

Bearing in mind the obligation of financial institutions to set up their operations within two hours (2hRTO), the document provides well-structured guidelines for a redesign aimed at achieving the adequate cyber resistance.

Some of the documents that are not binding, but are certainly worth mentioning in this context are:

- NIST Cybersecurity framework version 1.0 (a new upgraded version of this document is being prepared)
- Critical Security Controls version 6.0 of the Internet Security Center
- NIST 800-53 version 4

These documents are ripe and proven in practice and, unlike the international standards, they are subject to frequent alignment with the current trends so that they can effectively help in establishing a measurable cyber-resistance system, implementing the adequate security measures and achieving the desired level of security. In addition to all of the above, banks are exposed to many other standards and guidelines, such as the PCI-DSS standards or the new instructions that the SWIFT has imposed within the SWIFT Customer Security Program after the mentioned incidents occurred worldwide, with the clear goal, as the texts of the above mentioned laws, of raising the level of cyber resistance of all participants in a particular system.

Situation in the Republic of Serbia

A review of the legislation in the Republic of Serbia in the context of information security and financial institutions is outlined below in accordance with the dates and the order of adoption of regulations in this field. In 2010, the Government of the Republic of Serbia adopted the Strategy for the Development of Information Society in the Republic of Serbia until 2020. The Strategy defines information security as one of the priorities. This Strategy

se utvrđuju minimalni standardi i uslovi stabilnog i sigurnog poslovanja, a koji se odnose na upravljanje informacionim sistemima u bankama i drugim finansijskim institucijama. Ovom odlukom bankama i drugim finansijskim institucijama naloženo je da u skladu sa Odlukom dodatno urede sledeće oblasti:

1. Okvir za upravljanjem informacionim sistemom
2. Upravljanje rizikom informacionog sistema
3. Unutrašnju reviziju informacionog sistema
4. Bezbednost informacionog sistema
5. Upravljanje kontinuitetom poslovanja i oporavak aktivnosti u slučaju katastrofa
6. Razvoj i održavanje informacionog sistema
7. Poveravanje aktivnosti u vezi sa informacionoim sistemom trećim licima
8. Elektronske bankarstvo (odnosno elektronske usluge u poslednjoj verziji Odluke)

Oblast sajber bezbednosti nije direktno targetirana u ovoj odluci već se kao ključni segment uvodi obaveza uvođenje kontinuiranog procesa upravljanja bezbednošću informacionog sistema. Konkretni zahtevi koji su definisani u Odluci, a tiču se bezbednosti, jesu obaveza donošenja Politike bezbednosti, klasifikacija informacionih dobara, procena rizika i uspostavljanje odgovarajućih kontrola u skladu sa potrebama, određivanje osoba zaduženih za informacionu bezbednost, upravljanje korisničkim pravima pristupa, uspostavljanje sistema za nadgledanje i generisanje operativnih i sistemskih zapisa, obezbeđivanje integriteta podataka o platnim transakcijama, kao i obezbeđivanje adekvatne fizičke zaštite itd. Odluka je doživela izmene i dopune u februaru 2017. godine, a u cilju usklađivanja sa Zakonom o platnim uslugama što je za posledicu imalo izmene 9. Poglavlja, koje u poslednjoj Odluci ima naziv elektronske usluge i u kome se iste i uređuju. Novom odlukom bankama i drugim finansijskim institucijama omogućeno je odstupanje od obavezne dvofaktorske autentifikacije u različitim predefinisanim slučajevima i uz obavezno prethodno odgovarajuće obaveštavanje NBS. Oblast bezbednosti informacionog sistema delimično je pokrivena tekstom odluke, a čitav kontekst dokumenta svoje korene nalazi u seriji ISO 27000 standarda. Odluka je sa sobom je na scenu dovela i Centar za superviziju informacionih sistema NBS, koji je zadužen za kontrolu primene ovog dokumenta. Ovom odlukom u značajnoj meri podignuta je svest o značaju bezbednosti informacionih sistema i merama zaštite koje se koriste u okviru finansijskih institucija, a naročito u manjim finansijskim organizacijama.

Kako je u Republici Srbiji oblast informacione bezbednosti i dalje bila zvanično neuređena, država i resorna ministarstva su donošenje nacrta Zakona o informacionoj bezbednosti i javnu raspravu o njemu obavili u toku 2015. godine dok je sam Zakon stupio na snagu u junu 2016. godine (Službeni glasnik RS, br. 6/16). Zakon o informacionoj bezbednosti definisao je načela kojim se treba rukovoditi prilikom planiranja i primene mera zaštite IKT sistema, a to su:

1. Načelo upravljanja rizikom
2. Načelo sveobuhvatne zaštite
3. Načelo stručnosti i dobre prakse
4. Načelo svesti i osposobljenosti

Kao nadležni organ za poslove informacione bezbednosti u RS odgovorno je Ministarstvo trgovine, turizma i telekomunikacija. Zakon je takođe definisao i IKT sisteme od posebnog značaja, kao i mere zaštite za navedene IKT sisteme od posebnog značaja. Zakon uvodi i obavezu donošenja Akta o bezbednosti za IKT sisteme od posebnog značaja. U posebnom delu Zakon uređuje poveravanje aktivnosti u vezi sa IKT sistemom trećim licima, kao i obavezu obaveštavanja Nadležnog organa o incidentima u IKT sistemima. Zakon po ugledu na evropske standarde i direktive uvodi Nacionalni centar za prevenciju bezbednosnih rizika u IKT sistemima (nacionalni CERT), CERT republičkih organa, kao i mogućnost osnivanja posebnih centara za prevenciju bezbednosnih rizika u IKT sistemima (Poseban CERT) u okviru određenih pravnih lica, grupe pravnih lica, oblasti poslovanja i slično. Zakon takođe uređuje oblast kriptobezbednosti i zaštite od kompromitujućeg elektromagnetnog zračenja i ukazuje na poslove i ovlašćenja inspektorata za informacionu bezbednost

U toku iste godine, a u predviđenom roku, Vlada je na osnovu Zakona o informacionoj bezbednosti donela i prateće uredbe kojima je uredila sledeće oblasti:

facilitated the beginning of improvements in the legal and institutional information security framework in the RS.

The next important document for the financial institutions was published by the National Bank of Serbia in March 2013, which is the Decision on Minimum Standards for the Management of Information Systems of Financial Institutions (Official Gazette of RS, No. 23/13, 113/13 and 2/17). It prescribes the minimum standards and conditions for stable and secure business, which relate to the management of information systems in banks and other financial institutions. Thereby, banks and other financial institutions were forced to additionally regulate the following areas in accordance with the Decision:

1. The framework for information system management
2. Risk management of the information system
3. Internal audit of the information system
4. Information system security
5. Business continuity management and disaster recovery
6. Information system development and maintenance
7. Outsourcing of information system activities
8. Electronic banking (i.e. electronic services in the latest version of the Decision)

The cyber security area is not directly targeted in this decision, but the key segment introduces the obligation to implement a continuous information security management process. The specific, security-related requirements defined in the Decision are the obligation to adopt a Security Policy, the classification of information assets, the risk assessment and the establishment of appropriate controls in accordance with the needs, the appointment of information security personnel, the management of user access rights, the establishment of a monitoring system and a system for generating operational and system records, ensuring the integrity of data on payment transactions, as well as providing the adequate physical protection, etc. The decision was amended in February 2017, in order for it to be aligned with the Law on Payment Services, which resulted in the changes to Chapter 9, which in the last Decision refers to electronic services which are thereby regulated. According to the new decision, banks and other financial institutions are allowed to deviate from the mandatory dual-factor authentication in different predefined cases and with the obligatory prior notification to the NBS. The information security area is partly covered by the text of the decision, and the entire context of the document is based on the ISO 27000 series. The decision also involved the NBS Information Systems Supervision Department, which is in charge of controlling the implementation of this document. This decision has significantly raised the awareness about the significance of the information systems security and the measures of protection used within the financial institutions, especially in the smaller financial organizations.

Given that in the Republic of Serbia the information security field was still not officially regulated, the government and the competent ministries published the Draft Law on Information Security and the pertinent public discussion during 2015, whereas the Law itself came into effect in June 2016 (Official Gazette of the Republic of Serbia, No. 6/16). The Law on Information Security defined the principles that should be followed during the planning and implementation of the ICT system protection measures, which are:

1. Principle of risk management
2. Principle of comprehensive protection
3. Principle of expertise and good practice
4. Principle of awareness and competence.

The Ministry of Trade, Tourism and Telecommunications is the responsible body for information security in the Republic of Serbia. The law also defined the ICT systems of special importance, as well as the protection measures for the mentioned ICT systems of special importance. The law also introduced the obligation to adopt the Security Act for the ICT systems of special importance. In a separate section, the Act regulates the outsourcing of activities related to the ICT systems, as well as the obligation to notify the competent authority about the incidents in the ICT systems. Referring to the European standards and directives, the Law introduced the National Center for the Prevention of Security Risks in ICT Systems (National CERT), the CERT republic authorities, and the possibility of establishing special centers for the prevention of security risks in

1. Liste poslova u kojima se obavljaju delatnosti od opšteg interesa i u kojim se koriste IKT sistemi od posebnog značaja. U članu 2. ove uredbe pod tačkom 12. Poslovi finansijske institucije su u skladu sa zakonom kojim se uređuje Narodna banka, definisan nadzor odnosno kontrola nad njima je prepuštena Narodnoj banci u skladu sa važećim zakonom.
2. Mere zaštite IKT sistema od posebnog značaja u kojoj je bliže opisana 28 mera zaštite (videti tabelu 1):
3. Sadržaj Akta o bezbednosti, način provere i sadržaj izveštaja o proveri bezbednosti IKT sistema koji je bankama definisao sadržinu Akta i uveo obavezu godišnje provere usklađenosti sa aktom o bezbednosti IKT sistema, proveru adekvatnosti primene mera zaštite i procedura, kao i proveru bezbednosnih slabosti na nivou tehničkih karakteristika komponenti IKT sistema. Ovu proveru operator IKT sistema može da vrši samostalno ili uz angažovanje spoljnih eksperata.

Tabela 1 - Mere zaštite IKT sistema od posebnog značaja iz Zakona o informacionoj bezbednosti

Uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema
Postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja
Obezbeđivanje da lica koja koriste IKT sistem odnosno upravljaju IKT sistemom budu osposobljena za posao koji rade i razumeju svoju odgovornost
Zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema
Identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu
Klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. ovog zakona
Zaštitu nosača podataka;
Ograničenje pristupa podacima i sredstvima za obradu podataka
Odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža
Utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju
Predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti odnosno integriteta podataka
Fizičku zaštitu objekata, prostora, prostorija odnosno zona u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu
Zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem
Obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka
Zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera
Zaštitu od gubitka podataka
Čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema
Obezbeđivanje integriteta softvera i operativnih sistema
Zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema
Obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema
Zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove
Bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema
Pitanja informacione bezbednosti u okviru upravljanja svim fazama životnog ciklusa IKT sistema odnosno delova sistema;
Zaštitu podataka koji se koriste za potrebe testiranja IKT sistema odnosno delova sistema
Zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga
Održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga;
Prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama
Mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima

the ICT systems (Special CERT) within certain legal entities, groups of legal entities, business areas and the like. The Law also regulates the field of crypto security and protection against the compromised electromagnetic radiation and points to the duties and authorizations of the information security inspectorate. In the same year, within the prescribed deadline, on the basis of the Law on Information Security, the Government also enacted the following regulations, regulating the following areas:

1. Lists of jobs in which activities of general interest are performed and in which the ICT systems of special importance are used. Supervision over financial institutions is left to the NBS in accordance with the existing laws.
2. Measures for protection of the ICT systems of special importance in which 28 protection measures are described more closely (see Table 1 below).

Table 1 - Measures for protection of the ICT systems of special importance prescribed by the Law on Information Security

Establishment of an organizational structure, with the established tasks and responsibilities of the employees, providing the information security management within the ICT system operator
Achieving the safety of remote activities and the usage of mobile devices
Ensuring that the persons using the ICT system or managing the ICT system are trained for the work they perform and that they understand their responsibility
Protection against the risks arising from the changes in business or termination of work engagement of the ICT system operator employees
Identification of information assets and determination of responsibility for their protection
Classification of data so that the level of their protection corresponds to the importance of data in accordance with the principle of risk management referred to in Article 3 of this Law
Protection of data carriers
Restriction of access to data and data processing facilities
Approval of authorized access and prevention of unauthorized access to the ICT systems and services provided by the ICT system
Determining the responsibility of users to protect their own authentication assets
Predicting the proper use of cryptographic protection to protect the secrecy, authenticity, or integrity of data
Physical protection of facilities, premises or zones in which resources and documents of the ICT system are located and the ICT system data processed
Protection against loss, damage, theft or any other form of endangering the security of the assets constituting the ICT system
Ensuring the proper and safe operation of data processing facilities
Data protection and data processing tools against malicious software
Protection against data loss
Storing the data about events that may be important for the security of the ICT system
Ensuring the integrity of the software and operating systems
Protection against the misuse of technical security weaknesses of the ICT system
Ensuring that the activities of the ICT system audit have as little impact on the functioning of the system as possible
Data protection in the communication networks including devices and lines
Security of data transmitted within the ICT system operator, as well as between the ICT system operator and persons outside the ICT system operator
Information security issues related to the management of all stages of the lifecycle of the ICT system or parts of the system
Data protection used for testing the ICT system or parts of the system
Protection of funds of ICT system operators that are available to service providers
Maintenance of the contracted level of information security and the services provided in accordance with the terms and conditions agreed with the service provider
Preventing and responding to security incidents, which implies an adequate exchange of information on security vulnerabilities of ICT systems, incidents and threats
Measures to ensure business continuity in case of emergencies

4. Postupak dostavljanja podataka, listi, vrstama i značaju incidenata, kao i o postupku obaveštvanja o incidentima u IKT sistemu od posebnog značaja. Ovom uredbom banke su kao operateri IKT sistema od posebnog značaja dobili obavezu prijavljivanja određenih vsti incidenata i to sa rokom od najkasnije narednog dana od saznanja o nastanku incidenta. Navedene vrste incidenata banke prijavljuju centru za superviziju NBS na mail adresu supervizija. is@nbs. rs odnosno pisanim putem kako to ova uredba definiše.

Banke su kao finansijske institucije i u skladu sa Odlukom o minimalnim standardima NBS već dobrim delom uredile svoje informacioni sisteme, ali sa donošenjem Zakona o informacionoj bezbednosti dobile su detaljniji i opsežniji dokument kojim se preciznije definišu smernice i obaveze koje banke moraju primeniti u cilju zaštite svojih informacionih sistema. Uporednim analizama sa zahtevima koji proizilaze iz ovog zakona moguće je dobiti pregled oblasti u kojima je potrebno izvršiti korekcije ili potvrditi dobru praksu koju su finansijske institucije do tog trenutka sprovodile.

Nakon Zakona usledila je i objavljivanje Strategija informacione bezbednosti RS (Službeni glasnik RS br. 53/2017), u kojoj su objavljeni strateški pravci delovanja u ovoj oblasti. Kao opšti cilj Strategije definisan je razvoj i unapređenje informacione bezbednosti u Republici Srbiji i njeno održavanje na adekvatnom nivou. Kako je u prethodnom periodu Zakon o informacionoj bezbednosti definisao IKT sistem od posebnog značaja i mere zaštite koje ovi sistemi moraju da primenjuju, pored rada na primeni ovih propisa Strategija ukazuje na potrebu uvođenja posebnih programa na univerzitetima koji se bave informacionom bezbednošću, kao i kontinuirano obučavanje i usavršavanje zaposlenih na poslovima informacione bezbednosti u relevantnim institucijama. Za realizaciju navedenih ciljeva iz Strategije kao elemenat od ključnog značaja idenifikovana je saradnja između javnog sektora, privatnog sektora, nevladinih organizacija, akademske zajednice i drugih relevantnih činilaca. Kao osnove principe razvoje informacione bezbednosti Strategija navodi:

1. Informacionu bezbednost kao sastavni deo sveukupne bezbednosti
2. Informacionu bezbednost kao faktor od značaja za sve društvene činioce koji koriste IKT
3. Blagovremeno prepoznavanje rizika, preduzimanje preventivnih mera i efikasnu reakciju na incidente
4. Potrebu za uspostavljenjem i unapređivanjem redovne i efikasne razmene informacija o rizicima i incidentima na nacionalnom i međunarodnom nivou
5. Nastavak kontinuiranog razvoja sistema zaštite
6. Sistematsko podizanje svesti i unapređivanje znanja i veština kod svih kategorija građana
7. Uspostavljanje stalne saradnje između javnog i privatnog sektora

Kao prioritetne oblasti Strategija utvrđuje sledeće:

1. Bezbednost informaciono-komunikacionih sistema
2. Informaciona bezbednost građana
3. Borba protiv visokotehnološkog kriminala
4. Informaciona bezbednost Republike Srbije
5. Međunarodna saradnja

U okviru prioritetnih oblasti Strategija određuje različite strateške ciljeve koje detaljnije definiše i koji za cilj imaju razvoj i unapređenje informacione bezbednosti u definisanim prioritetnim oblastima. Iako se pojavila na kraju niza dokumenata, Strategija predstavlja krovni dokument kojim se potvrđuje spremnost države da se uredi oblast sajber bezbednosti.

Zaključak

Donošenjem u tekstu navedenih zakona i smernica Evropska unija i Republika Srbija pokušavaju da urede oblast sajber bezbednosti i bezbednosti informacionih sistema. Doneti propisi predstavljaju osnov i obezbeđuju polaznu tačku za ostvarivanje višeg stepena bezbednosti sistema, što će uz adekvatnu primenu u narednom periodu obezbediti poboljšanje opšte bezbednosne slike na polju sajber bezbednosti u čitavom regionu. Analizom u tekstu navedenih dokumenata možemo uočiti da postoji jasan trend usklađivanja domaćih zakonskih direktiva i pravilnika sa evropskim,

3. The content of the Security Act, the checkup methods and the contents of the report on the ICT system security. This regulation introduced the obligation of annual checks of compliance with the ICT system security Act, the adequacy of the implementation of protective measures and procedures, as well as the security weaknesses at the level of technical characteristics of the ICT system components. The ICT system operator can perform this checkup independently or by engaging external experts.
4. Procedure for submitting data, lists, types and significance of incidents, as well as the procedure for reporting on incidents in the ICT system of special importance. As a result of this regulation, banks, as operators of the ICT systems of special importance, became obliged to report on certain types of incidents, one day after they find out about the occurrence of the incident at the latest. These types of incidents are reported by banks to the NBS Supervision Department at supervizija.is@nbs.rs or in writing, as defined by this Regulation.

Banks, as financial institutions and in accordance with the NBS Decision on Minimum Standards, have already regulated their information systems, but with the adoption of the Law on Information Security, they got a more detailed and comprehensive document which defines more precisely the guidelines and obligations that banks must apply in order to protect their information system. A comparative analysis of the requirements arising from this law may provide an overview of the areas in which corrections are to be made or confirm the good practice that financial institutions carried out until that moment.

The Law was followed by the publication of the Information Security Strategy of the RS (Official Gazette of the RS No. 53/2017), which defined the strategic directions in this field. As a general goal the Strategy defined the development and improvement of information security in the Republic of Serbia and its maintenance at an adequate level. Given that in the previous period, the Law on Information Security defined the ICT systems of special importance and the measures of protection that these systems have to apply, in addition to the work on the implementation of these regulations, the Strategy underlined the need to introduce special programs at universities dealing with information security, as well as continuous training and training of the employees working in information security in the relevant institutions. The cooperation between the public sector, the private sector, non-governmental organizations, the academic community and other relevant stakeholders has been identified as an element of key importance for the realization of the goals stated in the Strategy. As the basic principles of information security development, the Strategy states the following:

1. Information security as an integral part of overall security
2. Information security as a factor of importance for all social factors using ICT
3. Timely recognition of risks, undertaking of preventive measures and effective responses to incidents
4. The need to establish and promote the regular and effective exchange of information concerning risks and incidents at the national and international levels
5. Continuous development of the protection system
6. Systematically raising awareness and advancing the knowledge and skills in all categories of citizens
7. Establishing continuous cooperation between the public and the private sector.

As priority fields, the Strategy determines the following:

1. Security of information and communication systems
2. Information security of the citizens
3. Combating high-tech crime
4. Information security of the Republic of Serbia
5. International cooperation.

Within the priority areas, the Strategy sets out the different, more precisely defined strategic goals which aim to develop and improve information security in the designated priority areas. Although it appeared at the end of a series of documents, the Strategy is an umbrella document that confirms the state's readiness to regulate the field of cyber security.

kao i da mere koje se navode u dokumentima predstavljaju ustaljenu međunarodnu praksu iz oblasti bezbednosti informacionih sistema.

Odgovor na pitanje da li su finansijske organizacije dovoljno bezbedne i koliki je stepen njihove sajber otpornosti ne nalazi se u donetim propisima već u načinu primene i posvećenosti koju organizacije iskazuju pri adresiranju ove oblasti

Sagledavajući trendove aktuelnih sajber napada, uočavamo veliki broj specifičnih sajber napada koji koriste maliciozni softver i specifične alate skrojene za konkretan napad i praktično napravljene za jednokratnu upotrebu, što otežava njihovu detekciju i prevenciju. Kako je trendom opšte digitalizacije izloženost finansijskih institucija sve veća, tako je i broj potencijalnih mesta koja napadači mogu kompromitovati takođe u porastu, što finansijske institucije dodatno stavlja pred nove izazove u pogledu adekvatne procene i prioritizacija uočenih sajber rizika. Posledice koje sajber napadi ostavljaju najčešće se ogledaju u direktnim, indirektnim finansijskim gubicima, kao i u značajnim reputacionim rizicima. Imajući u vidu veliki potencijal sajber rizika i mogućnost uticaja na kontinuitet poslovanja organizacija, ova vrsta rizika postaje segment koji ne sme biti ignorisan i skrajnut iz vidokruga top menadžmenta banaka. Jedan od preduslova uspostavljanja trajnog i efikasnog sistema sajber otpornosti banke svakako je i osvešćivanje top menadžmenta o ovim pitanjima i dobijanje njihove saglasnosti i podrške za uspostavljanje i održavanje čitavog sistema sajber otpornosti. Uspostavljanjem jasnih strategija, politika i procedura, kao i njihovom doslednom primenom banka jasno stavlja do znanja svesnost i potrebu da se sajber bezbednosti uzima kao jedan od ključnih faktora prilikom donošenja poslovnih odluka. U dinamičnom i svestranom sajber okruženju jedan od prvih izazova je identifikovanje realnih rizika kojima je banka izložena. Pravilnom procenom sajber bezbednosnih rizika kojima su izložene finansijske institucije omogućuje se adresiranje relevantnih rizika. Na osnovu odabira rizika koje žele da adresiraju organizacije imaju na rasploaganju odgovarajuće tehničke mere kojima se mogu umanjiti ili otkloniti uočeni rizici. Donošenjem okvira za sajber otpornost banke jasno pokazuju svoje ciljeve i projekcije, kao i trenutnu spremnost da uspešno upravljaju sajber rizicima u cilju ostvarivanja definisanih ciljeva. Kao neka od ključnih pitanja na koje banke u cilju uspostavljanja okvira moraju dati odgovore su:

- Koji procesi i koja dobra zahtevaju zaštitiu?
- Koje mere zaštite su na raspolaganju?
- Koje tehnike za identifikovanje incidenta su upotrebljene?
- Koji su odgovori na eventualne incidente?
- Koje su tehnike za oporavak kritičnih funkcija?

Odgovorom na data pitanja banke vrše selekciju i uspostavljaju adekvatnu odbranu svojih vitalnih servisa na najoptimalniji način fokusirajući trenutna sredstva na, po poslovanje, najbitnija mesta. Usvajanjem adekvatnog okvira obezbeđuje se i element merljivosti koji omogućava jasnije izveštavanje kako ka internim, tako i ka eksternim učesnicima u sistemu, a sve u skladu sa poslovnim ciljevima organizacije. I kao finalni cilj upotrebe sajber bezbednosnog okvira nalazi se sprovođenje integracije sajber rizika u opšti sistem merenja rizika, što stvara jasniju sliku i olakšava preciznije i efikasnije donošenje odluka na nivou čitavog sistema banke. Identifikacijom rizika i uspostavljanjem odgovarajućih mera zaštite banke su učinile značajan korak ka bezbednosti svojih sistema i podataka koji se u njima nalaze, ali da li su i postigle odgovarajući nivo sajber otpornosti? Aktuelna svetska dešavanja i trendovi jasno nam ukazuju na to da se proboji i najbolje obezbeđenih sistema ipak dešavaju, kao i da će se oni u budućnosti zasigurno dešavati, stoga je sledeća bitna oblast kojom se banke moraju posebno pozabaviti oblast detekcije i reakcije na incidente. Neka od pitanja na koja banke moraju imati odgovore su:

- Da li ste svesni načina na koji napadači mogu da kompromituju vaše sisteme?
- Da li ste u stanju da uradite adekvatnu rekonstrukciju događaja po otkrivanju upada u sistem?
- Da li postoje jasne procedure za slučaj incidenta?
- Da li vršite redovne treninge vaših timova za reakciju na incidente?

Analizom i davanjem odgovora na ova pitanja banke pokušavaju da smanje

Conclusion

By adopting the aforementioned laws and guidelines, the European Union and the Republic of Serbia are trying to regulate the field of cyber security and security of information systems. The adopted regulations represent the basis and provide a starting point for achieving a higher level of the system's security, which, provided the adequate implementation in the following period, will ensure the improvement of the general security image in the field of cyber security throughout the region. By analyzing the above documents, we can notice that there is a clear trend of harmonization of domestic legal directives and regulations with the European ones, and that the measures stated in the documents represent the consistent international practice in the field of information system security.

The answer to the question whether the financial organizations are safe enough and what the degree of their cyber resistance is, is not contained in the adopted regulations, but in the manner of implementation and commitment the organizations express when addressing this field. Examining the trends of the current cyber attacks, we notice a number of specific cyber attacks that use malicious software and specific tools tailored for a particular attack and practically made for disposable use, which makes their detection and prevention more difficult. As the trend of general digitalization increases the exposure of financial institutions, the number of potential sites that can be compromised by attackers also rises, which additionally forces financial institutions to face the new challenges in terms of the adequate assessment and prioritization of the observed cyber risks. The consequences that cyber attacks leave are most often reflected in direct and indirect financial losses, and in significant reputational risks. Considering the great potential of cyber risk and the possibility of its affecting business continuity, this type of risk becomes a segment that should not be ignored or left unnoticed by the top management of banks. One of the prerequisites for establishing a lasting and efficient system of cyber-resilience in banks is certainly the awareness of the top management about these issues, along with their consent and support for establishing and maintaining the entire cyber-resistance system. By establishing clear strategies, policies and procedures, and by implementing them consistently, the bank sends a clear message that it is aware of the need to take cyber security as one of the key factors in making its business decisions. In a dynamic and versatile cyber environment, one of the first challenges is to identify the real risks that the bank is exposed to. A proper assessment of cyber security risks to which financial institutions are exposed can help address the relevant risks. Based on the risk choices that the organizations want to address, they have the appropriate technical measures to reduce or eliminate the identified risks. By adopting the cyber framework for cyber resistance, the banks clearly demonstrate their goals and projections, as well as the current readiness to successfully manage cyber risks in order to achieve the defined goals. Some of the key issues that banks need to address in order to establish the frameworks are:

- Which processes and what kind of goods require protection?
- Which protection measures are available?
- Which techniques to identify the incidents have been used?
- What are the responses to potential incidents?
- What are the techniques for recovering critical functions?

By answering the given questions, banks select and establish an adequate defense of their vital services in the most optimal way by directing the current funds to the points most important for the business. The adoption of an adequate timeframe provides the element of measurability, which enables the clearer reporting to both internal and external participants in the system, all in line with the business objectives of the organization. The ultimate goal of using the cyber security framework is the integration of cyber risk into the general risk measurement system, which creates a clearer picture and facilitates the more precise and efficient decision-making at the level of the overall bank's system. By identifying the risks and establishing appropriate safeguards, the banks have made a significant step towards the security of their systems and the data contained

vreme potrebno za detekcije i reakciju na sajber incident, uspostave jasne definisane procedure i da na različite slučajeve incidenata imaju spreman odgovor. Kako stanje sajber bezbednosti nije tačka koju je moguće dostići i smatrati je završenim projektom, na bankama je izazov obezbeđivanja dovoljno reusrsa za kontinuirano praćenje, usklađivanje i prilagođavanje svog okruženja novim tipovima rizika koji se svakodnevno pojavljuju u sajber okruženju.

I dok pokušavamo da se izborimo za vidljivost u moru bitnih servisa i službi koje funkcionišu u banci u doba zahuktale digitalizacije, izazov adekvatnog pozicioniranja menadžmenata prema izazovima koje sajber okruženje donosi odrediće i sajber otpornost same banke i njenog poslovanja. Ipak imperativ bezbednog sajber okruženja kao preduslov za sticanje većeg poverenja i samim tim veće korišćenje digitalnih kanala podrazumeva uspostavljanje bezbednog okruženja za sve učesnike u sistemu i ostvarivanje nacionalne sajber otpornosti. Imajući u vidu opredeljenje države da krupnim koracima krene u proces digitalizacije, kao i tendenciju banaka da ovaj proces prate ako ne i da prednjače u njemu, pred sve nas se postavlja izazov uspostavljanja pouzdanog i bezbednog okruženja za postizanje zadatih ciljeva, jer samo bezbedno i pouzdano okruženje kome svi učesnici veruju jeste preduslov za uspešan razvoj i poslovanje.

Literatura / References

1. Cybersecurity Strategy of the European Union http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
3. G7 Fundamental Elements of Cybersecurity for the Financial Sector https://ec.europa.eu/info/publications/g7-fundamental-elements-cybersecurity-financial-sector_en
4. Principles for Financial Market Infrastructures https://www.bis.org/cpmi/publ/d101a.pdf
5. Guidance on Cyber Resilience for Financial Market Infrastructures (Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions) https://www.bis.org/cpmi/publ/d146.pdf
6. Strategija razvoja informacionog društva u Republici Srbiji do 2020. godine (Službeni glasnik RS br. 51/10 http://mtt.gov.rs/download/3/Strategija_razvoja_informacionog_drustva_2020.pdf
7. Strategija razvoja informacione bezbednosti u Republici Srbiji za period od 2017 do 2020. godine (Službeni glasnik RS br. 53/17)

therein, but have they achieved the appropriate level of cyber resistance? The current world developments and trends clearly indicate that intrusions into the best secured systems still occur, and that they will surely happen in the future, therefore the next important area which banks must specifically address is the detection and reaction to incidents. Some of the questions that banks have to answer are:

- Are you aware of the ways in which attackers can compromise your systems?
- Are you able to conduct an adequate reconstruction in case you discover an intrusion into the system?
- Are there clear procedures in case of an incident?
- Do you train your teams to respond to incidents?

By analyzing and responding to these questions, banks are trying to reduce the time needed to detect and react to the cyber incident, to establish clear-cut procedures and have a ready response in different types of incidents. As the state of cyber security is not a point that can be reached and considered a completed project, it is a challenge for banks to provide enough resources to continuously monitor, align and adjust their environment to the new types of risks that appear on a daily basis in a cyber environment.

And while we are trying to fight for visibility in the sea of essential services that function in a bank in these times of accelerating digitalization, the challenge of adequately positioning managers towards the challenges that the cyber environment brings will also determine the cyber resilience of a bank and its business. Nevertheless, the imperative of a secure cyber environment as a prerequisite for gaining greater trust and thus a greater usage of digital channels implies the establishment of a secure environment for all participants in the system and the achievement of the national cyber-resistance. Bearing in mind the state's determination to start the process of digitalization as a major step, as well as the tendency of banks to follow this process, if not to be at its forefront, we are faced with the challenge of establishing a reliable and safe environment for achieving our goals, because only the safe and reliable environment, which all participants believe in, is a prerequisite for successful development and successful business.

8. Odluka o minimalnim standardima upravljanja informacionim sistemom finansijske institucije (Službeni glasnik RS, br. 23/2013, 113/2013 i 2/2017) https://www.nbs.rs/internet/latinica/20/sis/min_standardi_upravljanja_IT_sistemom_p.pdf
9. *Zakon* o *informacionoj bezbednosti* (Službeni glasnik RS, br. 6/2016) http://mtt.gov.rs/download/1(2)/Zakon%20o%20informacionoj%20bezbednosti.pdf
10. Uredba o bližem sadržaju akta o bezbednosti IKT sistema od posebnog značaja, načinu provere i sadržaju izveštaja o proveri bezbednosti IKT sistema od posebnog značaja (Službeni glasnik RS, br. 94/2016)
11. Uredba o postupku dostavljanja podataka, listi, vrstama i značaju incidenata i postupku obaveštavanja o incidentima u IKT sistemima od posebnog značaja (Službeni glasnik RS, br. 94/2016)
12. Uredba o bližem uređenju mera zaštite IKT sistema od posebnog značaja (Službeni glasnik RS, br. 94/2016)
13. Uredba o utvrđivanju liste poslova u oblastima u kojima se obavljaju delatnosti od opšteg interesa i u kojima se koriste IKT sistemi od posebnog značaja (Službeni glasnik RS, br. 94/2016)