# Research methods in information technology and it management

According to BDO, India, as rapid intensify in the usage of digital channels such as internet banking, digital wallets, mobile banking, ATM centres which leads to the enlarge in exposure and thereby cyber-attacks which further may point to financial and reputational drops. Banks may lose the customer confidence which can further expand the impact. The key influencers which makes it compulsory for the banks to lend in security are:

- Increase in financial data drops including card data, personal identifiable information etc.
- Unauthorized access to bank network and systems.

For Raiffeisen having all activities involving security in-house is neither economical nor effective. With associate explosion of data and threats its punishing to remain up date for in-house employees and it had been first challenge. Liberating up time for it innovation was the second challenge. With the overwhelming majority of Raiffeisen’s it department that specialise in developing and implementing new product and services it would be a pity to position that continuous modernization on hold due to the large burden of maintaining to this point with the latest evolutions in security jean-luc-martino federation notes. It is abundant worthier to travel away the foremost vital chunk of the work to those partners United Nations agency have gathered years of expertise and knowhow one issue we have an inclination to simply cannot build up as a company on our own. For additional sensible and economical security and to unencumber time for it modernization Raiffeisen created the set up of action decision to supply security observance to sensible players.

With increasing risks of cyber threats, banks are facing an unprecedented challenge of data breaches and are therefore strengthening their cyber security postures. The following are the noticeable trends in banking industry from cyber security point of view:

- Financial sector faced almost three times the cyber-attacks as compared to that of the other industries;
- Data breaches (both internal through fraud and external through cyber criminals) leads to the exponential rise in costs;
- There is an escalate in biometrics and tokenization as banks have begun to recognize that in addition to be a solution for payments these controls are also useful in security the sensitive data;
- Customers are using biometrics for banking activities such as authentication for mobile banking, transaction at ATMs and payments;
- With digital channels becoming the preference choice of customers for banking services, banks will also need to leverage advanced authentication and access control processes, without any compromise to customer experience.

Raiffeisen started technique to accumulate a SIEM system combining with IBM. The banks new core banking platform that was launched four years a gone has IBM infrastructure beneath the hood. To boot inside the context of cybersecurity IBM was already involved in Raiffeisen’s network security through delivering intrusion detection and hindrance ids-ips services to Raiffeisen from its security operations centre soc IBM delivered its intelligence activity answer IBM QRadar SIEM and manages this technique for Raiffeisen in its Luxembourg soc.

The centre is co-operated with Sogeti and equipped to fulfil the rigorous compliance desires of Luxembourg’s cash sector. They monitor the Raiffeisen it atmosphere victimization QRadar’s analytical capabilities that finally ends up in fundamental measure 24/7 harvest and correlating of logs to note security breaches. Once associate degree intensive pre-selection alone relevant incidents square measure sent back to the Raiffeisen it and employees. Which implies IBM excludes among various things false positives from the incident outline.

While each bank thinks distinctively on adopting various considerations it is imperative to assume that the theme remains the same for various banking channels.

## Internet Banking

Security controls like multi factor authentication, creation of strong passwords, adaptive authentication, image authentication, etc. can be considered.

## Mobile Banking

It should be ensured that mobile applications are up to date and should be tested. Latest hardening standards could be implemented.

Wallet Transactions: Awareness material on Phishing, Malware attacks, vishing and social engineering, Password security etc. should be incorporated.

## ATM Security

Biometrics like eye-retina, voice scan or fingerprint scan should be introduced by Banks.

## Unified Payment Interface

Banks need to think through their security strategies, governance models and predictive controls to build a secure UPI (Unified Payment Interface) environment that ensures a seamless user experience and at the same time balances security risks.

According to Security Central, New Zealand, to achieve computer security goals, it needs own tight 5. It takes the time to educate people about these 5 computer security activities and it will help protect home devices or small business systems from common cyber incidents. Below is the list of tight 5.

- Think before you click
- Update everything
- Backup files
- Secure wireless network
- Use strong passwords

According to Raiffeisen. IBM Security QRadar. Luxembourg. 2018. The very real problem that cybersecurity poses is only going to grow as our lives become increasingly dependent on technology, and systems become more interconnected. By 2020 the number of connected devices – from smartphones and tablets, to autonomous cars and smart home devices – is set to reach 20 billion across the globe, according to research from technology consultancy Gartner. Such an environment creates a plethora of opportunities for hackers to infiltrate and exploit weaknesses.

Financial firms, as operators of critical and global infrastructure, are not only exposed to some of the greatest cybersecurity risks this interconnected

environment creates, they are (and must by necessity be) at the forefront of efforts to tackle them. They are key for ensuring financial stability as suggested by FinTech Futures.

According to IBM Security. 2016. IBM intelligence and Analytics Whiteboard, IBM QRadar SIEM allow security analyst to watch anomalies, uncover advanced threats and remove false positives in amount. By strengthen log events and network flow info from ton of devices, endpoints and applications distributed throughout network, QRadar accelerates incident analysis and repudiation. QRadar SIEM is obtainable on zone associate degrees in an extremely cloud surroundings.

IBM QRadar is associate enterprise security data and event management product as SIEM. It collects log information from associate enterprise, its network devices, host assets and operational systems, applications, vulnerabilities, and user activities and behaviours. IBM QRadar then performs amount analysis of the log information and network flows to identify malicious activity so it Is stopped quickly, preventing or minimizing hurt to the organization.

In addition, IBM QRadar can collect log events and network flow information from cloud-based applications, and it’s deployed as a SaaS providing on the IBM cloud where preparation and maintenance is outsourced.

In addition to the essential SIEM capabilities that enterprise SIEM product typically provide, IBM QRadar SIEM to boot offers support for threat intelligence feeds. Optionally, associate IBM QRadar SIEM can have a license extension purchased that allows use of IBM Security X-Force Threat

Intelligence, that identifies subject area addresses and URLs that area unit relating to malicious activity. for each well-known subject area address or uniform resource locator, the threat intelligence feed includes a threat score and sophistication, which can facilitate a company higher analyse and grade threats. IBM QRadar SIEM is a component of the IBM QRadar intelligence Platform, that has modules for risk management, vulnerability management, forensics analysis and incident response. The advantages of exploitation IBM QRadar are listed below:

- Reduce the impact of threats with intrinsically analytics that accelerate SecOps workflows
- Accurately observe threats: Receive knowledge from anyplace and apply advanced analytics. observe and rank important threats whereas reducing false positives.
- Gain intelligent insights: See the end-to-end chain of events concerned in an exceedingly threat, mechanically connect connected incidents and augment investigations with AI (AI).
- Act with speed: Deploy quickly, observe threats in period and accelerate investigations by fifty times to accelerate security operations – even with restricted resources.
- Provide close to period visibility: Capture log event and network flow knowledge in close to real time and apply advanced analytics to reveal security offenses.
- Reduce and rank alerts: Focus security analyst investigations on a brief, manageable list of suspected, high likelihood incidents.

- Optimize threat detection: Sense and track vital security incidents and threats with supporting knowledge and context for easier investigation. produce careful knowledge access and user activity reports.
- Easily manage compliance: accommodates internal structure policies and external rules by providing several customizable reports and templates.

The key Feature of IBM QRadar square measure listed below:

- Sense and sight fraud, business executive and advanced threats
- Perform immediate event standardization and correlation
- Sense, track and link vital incidents and threats
- QRadar SIEM is deployed on premises or in cloud environments
- Add additional storage and process for quickly and inexpensively
- Implementation is provided for data-privacy policies
- Enable threat-prevention collaboration and management
- Integrate with numerous IBM and non-IBM stock

To justify the IBM QRadar software below the detail information of Cargills bank to make their bank more secure.

Cargills Bank wanted to enhance its existing defensive cyber security capabilities, improve monitoring and implement stronger preventive protocols to guard against sophisticated threats. The bank is using IBM QRadar SIEM, an industry leading security intelligence platform, with Watson cognitive capabilities for early detection and classification of cyber threats.

The challenges made by bank and achieved the result by securing. Cargills Bank, a new banking entrant in Sri Lanka, is known for its unconventional

business model built on access, convenience and inclusivity. Building on the rich heritage of the 174-year-old Cargills brand, the bank has a growing network of branches and over 340 access points at Cargills Food City outlets across the country.

“ As the newest bank in the country, without a traditional brick and mortar legacy, we are a true digital bank while being able to leverage supermarket banking through the retail footprint of Cargills Food City,” says Rohan Muttiah, Chief Operating Officer. “ The Cargills value chain is arguably the largest in the country, thereby providing a unique business eco-system for banking services.”

Security has been topping of mind for the bank, as sophisticated cyberattacks and a constantly changing threat landscape continue to multitude financial institutions across the globe. Cargills Bank wanted to enhance existing defensive capabilities, with improved monitoring and stronger preventive protocols to defend against sophisticated threats. The bank also wanted a solution to help security analysts to keep up to date on the endless amount of security data, including data generated from internal systems as well as threat intelligence, security research papers, security blogs, websites and other external sources of information required to analyse threats.

“ We are committed to enhancing our customers’ digital banking experience while being sensible of emerging security threats. With cybercrime becoming more organized and sophisticated, it is imperative to deploy highly adaptive

prevention, detection and response capabilities based on proven technology," Rohan Muttiah adds.

The benefits for bank by using IBM QRadar are: Speeds: the process of detecting and accurately identifying cyber threats and alerts Guards: against sophisticated threat incidents with stronger preventive protocols Transforms: millions of security documents into actionable intelligence relevant to specific threat.

IBM QRadar SIEM offers a regular, appliance-based approach to SIEM which will scale to satisfy the event log and network flow observance and analysis wishes of most organizations. Additional, integrated modules for risk and vulnerability management, forensics analysis of packet captures, and incident response (from the recently nonhereditary Resilient Systems technology) are out there as decisions, though they are not swallowed. The IBM QRadar SIEM jointly supports IBM X-Force Threat Intelligence and different third-party threat intelligence feeds via STIX and TAXI to spice up threat detection. Organizations curious concerning interested in interested by evaluating enterprise SIEM product have to be compelled to gather further knowledge about IBM QRadar SIEM to help ensure if it meets their requirements.