WHITE PAPER
MAY 2020

TAILORING CYBERSECURITY
FOR BANKING SECTOR

ults

www.ults.in

Author : **Vinod T** - Head, Cybersecurity CoE, ULTS
Co-Author : **Praveen C** - Cybersecurity Analyst, ULTS

TABLE OF CONTENTS

INTRODUCTION

> Financial Institutions are 300 times more vulnerable than the other sectors
>
> - BCG

Cyber risks in the banking sector have increased exponentially as banks have moved digital to improve customer convenience, stay afloat in the competitive landscape and reduce the transaction cost. The use of advanced technologies and digitisation creates an abundance of confidential and useful data at every touchpoint. This massive confidential information and the data that resides in the bank's data centres, applications and the network could be exploited for all wrong reasons. The number, frequency and impact of cyber incidents/attacks have increased manifold in the recent past.

The cyber attackers are motivated due to the active and vulnerable network consisting of customer sensitive information, third party applications and internet banking thus turning the banking sector as a potential target. The Cyber risk has emerged as a systemic risk concern for the banking sector, following the recent cyber incidents:

1. **Malware attack on Indian ATMs (23 Sep 19):** North Korean cyber attackers launched a malware named as ATMDtrack to steal payment information from Indian ATMs and banking institutions.

2. **SBI Breach (4 Feb 19):** It is reported that the vulnerability of the servers of the bank was exploited to gain the access to the system and steal personal information of approximately 422 million customers'.

3. **Attack on Cosmos Bank (11 Aug 18):** Cosmos Bank which is the second biggest cooperative bank in India lost ₹94 Crore through an organised cyber attack.

4. **Southeast Asian Banks Credit Card Breach (6 Mar 20):** This data breach resulted in stealing of over 2,00,000 credit card details of top banks in Singapore, Malaysia, Philippines, Indonesia and Thailand.

5. **DDoS attack on Australian Banks (25 Feb 20):** Distributed Denial of Service attack was launched on major Australian banks and financial institutions and requested payment in cryptocurrency to stop the attack.

Evolution of attack:
The sophistication of cyber attacks is increasing as the banking sector is continuing to learn and defend cyber attacks. This is making hackers explore new attack vectors and techniques. They are continuously now seen targeting the bank's core systems.

2006 Trojans (ZeuS, Dridex, Shylok)

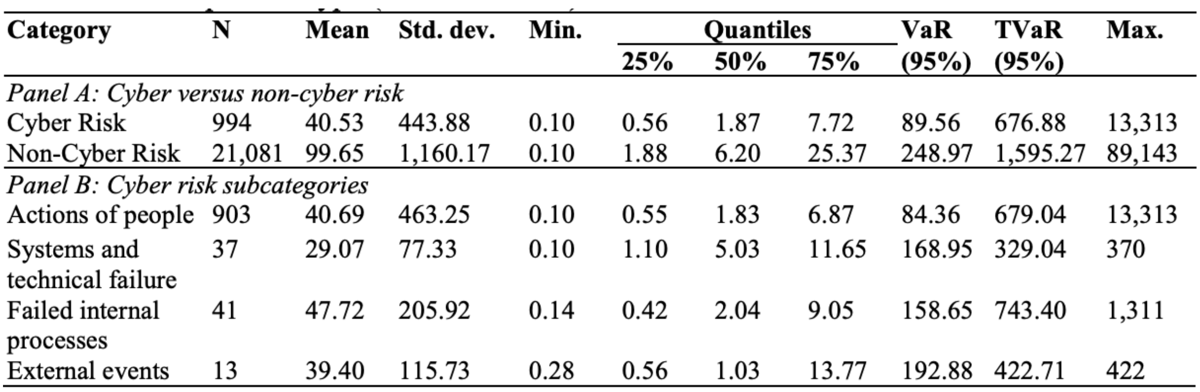
2014 ATM Network Attacks (Carbanak Malware)

2018 SWIFT Payment Attacks (Lazarus, ATMDtrack)

2019 CBS, 3rd Party Applications Social Engineering

Based on research by Christian Biener, Martin Eling and Jan Hendrik on cyber risks, it was observed that most of the cyber risk incidents have a human element to it. Cyber attacks, Personal Identifiable Information (PII) and credential thefts, human failures are the main sources of cyber risk, while the other categories such as external disasters are very rare.

The level of technology adoption is different across the banking sector; there are banks with a range of state-of-the-art digital products and banks that rely on legacy systems. The complexity of its Information Technology (IT)/Information Security (IS) systems, nature of digital products offered, would mean that the concerned organisation has to identify the vulnerabilities, securely handle the confidential information of customers and ensure continuity of business. This would mean having an information security policy in place and complying with the standards like ISO 27001, PCI-DSS or RBI Cybersecurity guidelines is essential.



Category	N	Mean	Std. dev.	Min.	Quantiles			VaR	TVaR	Max.
					25%	50%	75%	(95%)	(95%)	
Panel A: Cyber versus non-cyber risk										
Cyber Risk	994	40.53	443.88	0.10	0.56	1.87	7.72	89.56	676.88	13,313
Non-Cyber Risk	21,081	99.65	1,160.17	0.10	1.88	6.20	25.37	248.97	1,595.27	89,143
Panel B: Cyber risk subcategories										
Actions of people	903	40.69	463.25	0.10	0.55	1.83	6.87	84.36	679.04	13,313
Systems and technical failure	37	29.07	77.33	0.10	1.10	5.03	11.65	168.95	329.04	370
Failed internal processes	41	47.72	205.92	0.14	0.42	2.04	9.05	158.65	743.40	1,311
External events	13	39.40	115.73	0.28	0.56	1.03	13.77	192.88	422.71	422

Fig: Losses per risk type (in million USD).
Source: Research paper Insurability of Cyber Risk: An Empirical Analysis.

AN OVERVIEW OF CYBER ATTACKS TARGETED AT BANKING INSTITUTIONS

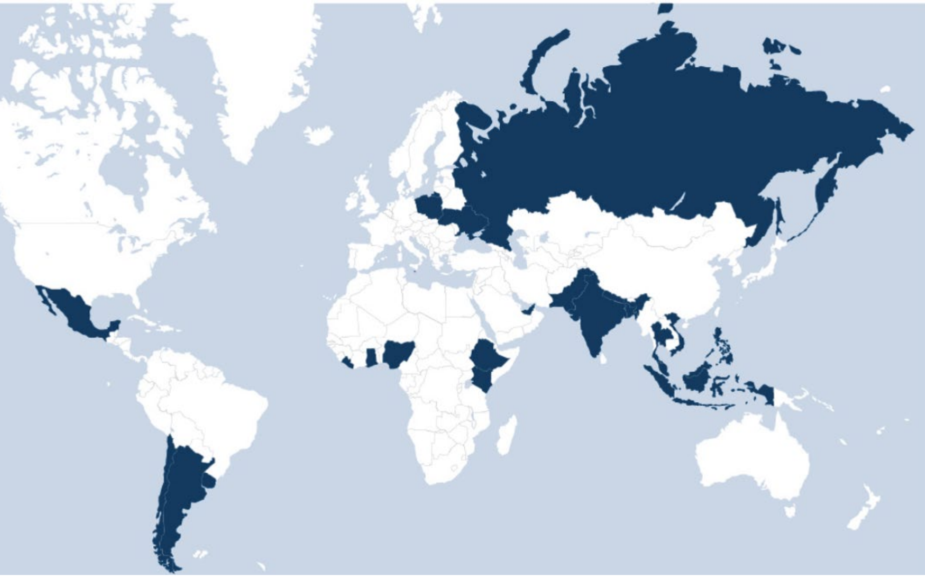
The complex business and financial operations often connect directly to digital and physical security concerns and vulnerabilities.

The digitisation in the banking sector has expanded the attack surface resulting in an increase in the threat landscape. In addition to the cyber hacktivists, the state-sponsored group and the thriving professional cyber criminals on the dark web throw open challenges to the banking institutions, thereby, increasing the need to protect the cyber infrastructure and their customers. As the cybersecurity landscape becomes more diverse and challenging, no organisation can say that they are free from any kind of cyber security breach.

The increasing trends among the cyber security threats are as follows:

1. The attackers are now equipped with the latest tools and techniques to exploit a vulnerability and leave the area with minimal or nil traces. As mentioned earlier, the human element remains as the weakest link of the chain and this has motivated the attackers to adopt smart and sophisticated techniques to exploit them.

2. The attackers have been researching and building advanced capabilities to attack the core banking software (CBS), ATM switches, RTGS/NEFT, mobile banking, internet banking and 3rd party payment gateway systems.



The geolocations of attack to the payment systems across the world show that Latin America, Africa, Asia are relatively less matured with respect to the cybersecurity defensive measures.

Source: Carnegie Endowment for International Peace

3. The ever-growing cyber criminal market place in the dark web offers tools and Personal Identifiable Information (PII) like Aadhaar card details, credit cards, banking credentials, KYC details to facilitate cashing-out and money laundering.

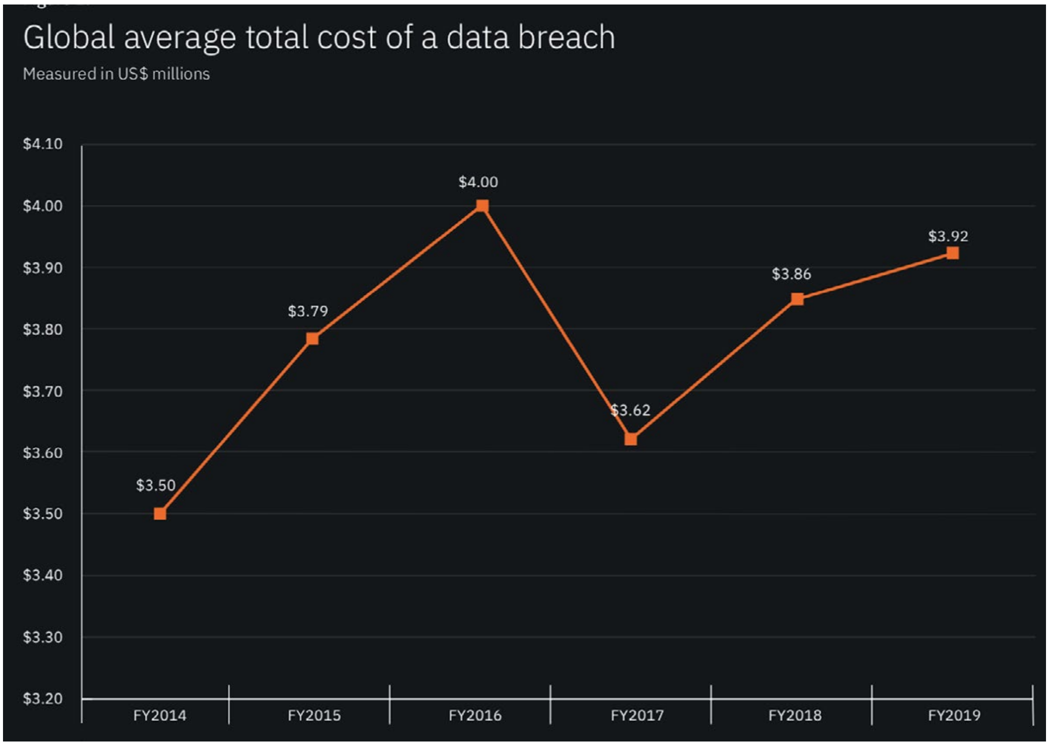
4. The boundaryless cyber crime landscape, nascent cyber law and the loosely knit treaties among the countries make it all a challenge to trace out the cyber criminals and take appropriate legal action.

As per a research conducted by the Ponemon Institute, the average total cost of a data breach has increased from $3.86 million to $3.92 million. The average cost per compromised record too has seen an increase from $148 to $150.

The total cost of a data breach for the financial sector is $5.86 million and the average cost per breached record is $210. Researchers found that over time, the cost of a data breach has steadily increased.

- The lifecycle of a data breach in 2019 was 279 days longer than the 2018 lifecycle of 266 days.
- Malicious attacks had a 12.5%, 314 day longer lifecycle.
- A life cycle that is longer than 200 days cost $4.56 million vs $3.34 million for a breach that is shorter than 200 days.

> An average enterprise uses 76 security products to secure their network - they need to work together.
>
> - IBM Security


Global average total cost of a data breach

Measured in US$ millions

Source: Cost of data breach report 2019 - Ponemon Institute.

STANDARDS AND BEST PRACTICES

Accreditation/adoption of information security standards brings some of the best practices to secure the banking sector. Adopting any or combination of the information security standards like ISO 27001, RBI Cybersecurity Guidelines, PCI-DSS, COBIT, NIST can help to improve the security posture of the organisation and minimise the risk. A security breach can also lead to a legal or business continuity implications.

When banks and financial institutions comply with information security standards and more importantly the RBI Cybersecurity Guidelines, they will be assured of:

- All the required knowledge, information to keep the data protected
- Data integrity and availability
- Protection of information and communication technologies
- Protecting the assets of the organisation
- Disaster recovery and business continuity
- Compliance to legal and regulatory standards
- Defined information-handling roles and responsibilities
- Avoiding financial losses resulting from a security breach
- Protection of facilities, offices and working environment
- Confidentiality, credibility and trust
- Greater awareness of security across the organisation
- Prevents confidentiality breaches and data leakage
- Fast reaction and disaster recovery
- Meeting international benchmarks of security
- Best practices to ensure highest level of security for online & mobile banking

RISKS ASSOCIATED WITH BANKING SECTOR

The disruptive innovation in the banking sector to keep pace with the ever-growing customer expectation and cost optimisation has introduced complexities into the digital ecosystem. The complex digitised environment comprising internet banking, mobile banking, core banking, ATM switches, 3rd party applications, cloud technology and more has introduced vulnerabilities to the ecosystem thereby broadening the attack surface.

A few major attack vectors are described as follows:

1. Account takeovers
2. Fraudulent payment systems
3. ATM skimming
4. Compromise at the Point of Sale
5. Internet and mobile banking exploitation
6. Cloud infrastructure becoming an easy target of the malicious actors
7. Social engineering leading to ransomware attacks
8. Easily exploitable IoT devices and physical security
9. Lack of cybersecurity awareness and security culture

APPROACH

The cybersecurity strategies of the banking institution should be to protect its critical assets and increase digital resilience. The cybersecurity approach should address cybersecurity strategy, governance, risk management and culture. This cybersecurity strategy should necessarily comprise people, process and technology and can be achieved through a holistic approach.

Steps	Objective	Actions
Identify risk appetite	Prioritisation of identified risks	Work with top management to create a list of critical assets, known risks and potential risks. Understanding of the risk appetite of the organisation and classifying the risks accordingly. Assessing of existing controls and vulnerabilities
Analysis and Evaluation	Prioritise areas for mitigation, starting with the most likely scenarios that will have the biggest negative impact	Expert analysis to evaluate each risk with likelihood of occurrence and potential impact including regulatory, operational & financial impacts. (Service disruption, Data leakage, Cyber fraud, Physical security)
Treatment	Identification and mitigation of vulnerabilities and exploits	IS Policy Audit, Vulnerability assessment, Simulate attack conditions, Mitigation of the top risks, Check for the residual risks if any and compare with the organisations risk appetite.
Monitoring	Monitoring of the risks through different dashboards for IT, business and management	Creation of separate dashboards

HOW AND WHAT TO PROTECT

The banks should consider the following level of preparedness:

1. By remaining secured against known threats through risk management, preventive controls and policies
2. Remain vigilant to detect emerging threats and anomalous patterns amid the highly complex digital environment; and
3. Being resilient to enable the organisation to recover from attacks as quickly as possible.

A cyberattack can cause irreparable damage to an organisation's reputation and lose customers' trust in its business. Safeguarding of the data and cyber infrastructure requires a strong cybersecurity strategy.

1 Information Security Management system

Governance, Risk and Compliance Audits based on ISO 27001 / RBI Cybersecurity / PCI-DSS Framework

2 Network management and Security

Network design validation, ASLC*

Network segmentation recommendations - Trusted, Un Trusted, DMZ

Perimeter Security - Firewall rules, Backdoor entries, Wireless Access,

Application security audit

3 Secure configurations

Assess the security configurations for:

Computing Devices & Applications: Servers, Application and Database, etc.

Networking Device: Switches, Routers

Perimeter Security Devices: Firewall, IPS, IDS, UTM

Endpoint Devices: Desktop, Laptop, Mobiles, IoT Devices

4 Baseline security controls

User Access Controls/Management

NAC, DLP (Data Leakage Prevention)T

Anti-Phishing

Audit Logs - Server, Firewall

Incident response process validation

5 Periodic Testing

Periodic Vulnerability Assessment - Penetration Testing of internet facing applications, Servers, Network components.

VA PT of critical applications and network elements once in 6 months.

6 Incidence response and Continuous Surveillance

Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital Forensics to reduce the business downtime and bounce back to normalcy.

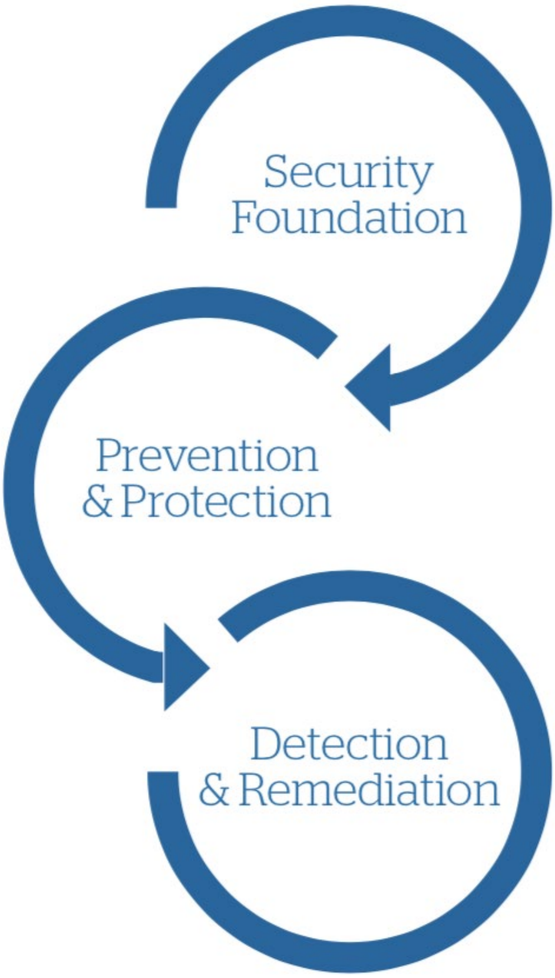
CYBERSECURITY FOUNDATION

Cybersecurity framework for bank shall cover:

CYBERSECURITY FRAMEWORK		
Cybersecurity Strategy	IT Architecture	Continuous Surveillance
Cybersecurity Policy	Network and Database Security	
Risk/Gap Assessment	Cybersecurity Preparedness Indicators	Reporting Cyber Incidents
Cyber Crisis Management Plan	Cybersecurity Awareness	

PREVENTION & PROTECTION

Once a strong security foundation is established, prevention & security controls will avert the threat before it occurs and the protection & security control takes over when prevention fails.



What are the protection controls?

Protection controls are a combination of security equipment like Endpoint threat detection and response EDR, Anti-malware, e-mail security controls, IAM, C-SoC and information safety standards like ISO27001, RBI cybersecurity guidelines that are used to defend against and eliminate threats.
Prevention and Protection are different, but both must be used simultaneously to secure banks from possible threats.

DEFENCE-IN-DEPTH:

The best way to secure the data is to deploy multiple defensive measures. Multiple layers will be of use in case of a failure to one layer. In case of a failure to one layer the other layers will be able to handle the threat to a certain extent.

This is the reasoning behind defence-in-depth security. A security strategy of this kind implements numerous layers of defense against threats and can include:

- Network security
- Endpoint security
- Application security
- Administrative controls
- Physical barriers
- Perimeter security

Security Baseline	Controls	Description
Security Foundation	**Build a cybersecurity culture**	Cybersecurity culture at the workplace amounts to the promotion of safe cybersecurity practices that integrate seamlessly with people's work. It will make employees aware of cybersecurity threats and make them amend their behaviour accordingly to mitigate potential threats. Starting from the top management and then cascading to all the employees, through awareness sessions, training & workshops can help to create a security culture.
Security Foundation	**Develop an end-to-end cybersecurity strategy**	1. Identify the critical assets, the crown jewels. 2. Devise a strategy to protect them 3. Implement prevention security controls 4. Comply to information security standards
Protection and Prevention	**Secure the network infrastructure**	Secure the network infrastructure 1. Edge environment - Firewalls, IDS/IPS, Routers 2. Computing environment - Servers, Cloud 3. Endpoint environment - Laptops, Desktops, Mobile devices 4. Third party environment
Protection and Prevention	**Network Architecture Security Review (CIS Standard)**	Network architecture security review is to identify weaknesses, gaps in existing security controls and compare their alignment with the organisation's security objectives.
Protection and Prevention	**Security Controls**	Some security controls 1. DLP - Data loss prevention 2. Encryption of data 3. Protection from DDoS attacks 4. Identity Access Management 5. Patch management 6. User access control, Least privilege
Protection and Prevention	**Vulnerability Assessment and Penetration Test**	The network & app security audit will help to determine the effectiveness of security and to resolve underlying security issues. VAPT audits are critical to understanding how well the organisation is protected against security threats - internal or external.
Detection and Remediation	**Surveillance & Incident response**	1. MSSP - Managed security services 2. MSP - UL Managed Security Platform 3. Digital surveillance - CSoC (Cybersecurity Operations Center) 4. Periodical VAPT - Quarterly remote test and Half yearly remote and onsite 5. Incident response 6. Cyber Insurance

CONCLUSION

This paper provides necessary insights for the management to get the basics of cybersecurity threats, necessary governance and essential tools which any banking institutions may want to deploy. Banks must have a periodic assessment and regular rehearsal to its response and recovery plan.

At ULTS, we believe that we cannot delay collectively addressing the evolving cybersecurity threats facing us.
ULTS has been at the forefront of efforts to improve cybersecurity across the digital continuum. We offer a unique understanding of the gravity of the cybersecurity challenges and the changes in the threat landscape that the financial sector, government and consumers are facing. Countering these increasingly sophisticated threats to networks, intellectual property, and privacy requires to develop, continuously refine and practice cybersecurity as a process, not to be treated as an end state. Cybersecurity is a journey, not a destination!

REFERENCES:

Ponemon Institute research Cost of a Data Breach Report highlights - 2019

RBI Cybersecurity guidelines for the banking sector

ISO 27001 Handbook

Baldridge Cybersecurity excellence builder, V1.1 2019.

White paper on Insurability of Cyber Risk: An Empirical Analysis by Christian Biener, Martin Eling, Jan Hendrik Wirfs, University of St. Gallen

IMF WP on Cyber risk for Financial sector: A Framework for quantitative assessment, by Antoine Bouveret

White paper on Cybersecurity & Financial Stability by Martin Boer & Jaime Vazquez, Institute of International Finance

White paper on Cyber risk management and 10 essential security tools by Bharat Panchal, NPCI

Cyber risk measurement and holistic cybersecurity approach by Jim Boehm, Peter Merrath, Thomas Poppensieker, Rolf Riemenschnitter, and Tobias Stähle, McKinsey & Company

2019 Banking and capital markets outlook by Deloitte Center for financial services

8 biggest data leaks of 2019 that hit Indian users hard - The Economic Times. 17 Dec 2019

ABOUT ULTS

Rooted in the principles of parent organisation Uralungal Labour Contract Cooperative Society (ULCCS) to diversify and grow, UL Technology Solutions (ULTS) was established as a new generation face of the very same society. In those terms, we are distinguished as a Cooperative Corporate and very different from any other competitors.

The idea behind the venture was to give educated youth, the second generation of the labourers who made ULCCS an icon to follow, contemporary job opportunities in a changing world.

Following the footsteps of ULCCS, ULTS also gives priority to Trust, Timeliness and Quality delivery. Started in 2011, the organisation stands for exponential values through extreme automation.

ULTS is specialising in disruptive technology including Blockchain, IoT, AI & Analysis, GIS, ERP, IMS and Cyber Security along with Web and Mobile applications development.

Currently, the organisation offers a unique mix of traditional values and modern technological insights into its services and helps to formulate and implement comprehensive solutions for its clients.

ULTS expects to flourish as a major IT Company across the country in the next five years. Currently, the company has a staff strength of more than 450 with offices in UL Cyber Park, Kozhikode, Thiruvananthapuram, Kochi, New Delhi and Bengaluru.

To move forward with securing your banking operations, contact **sales@ults.in**

ULTS, UL CyberPark, Nellikode P.O,
Kozhikode - 673 016, Kerala, India.

ults

www.ults.in

Connect with us: