EXCELIC INFOTECH

A Data Protection Company

Information Security For Finance Industry

About Excelic

For some, the path to excellence is a steady march. For others, it unfolds through bursts of innovation. But for the best of the best, it's both, disciplined improvement initiatives, marked by powerful leaps and breakthroughs. As the world's largest professional services firm, we help organizations build value and excellence by uncovering insights that create new futures and doing the hard work to improve performance.

Excelic's Profile - Overview

Excelic – specialist risk and compliance firm with expertise in IT risk management

Flexible "On Demand" Governance and Risk Consulting Services, Satellite presence in Middle East, India, Europe

Ex **Big 4 leadership** with combined 250+ years of professional services experience.

Risk and compliance expertise across industries, risk consulting services & operations; serving more than **100 clients across the globe**

15+ experts specialized in IT solutions with CISA, CISSP, ISO 27001, ISO 22301, OSCP certifications

15+

Seasoned Risk & Audit Professionals

10+

IT Risk Management Professionals

15+

Cyber Security Professionals

IT RISK MANAGEMENT TEAM

- Techno functional team to conduct application reviews.
- Pool of CISA, CISSP, CISM, OSCP, CEH, ISO27001 LA, CRISC and other relevant certified professionals
- Team with a good mix of industry and consultancy background
- Team with technical expertise in networks and infrastructure reviews
- Methodology aligned to the ISO 27001/ COBIT / ISF framework
- Large repository of technology risk and controls database
- Audit methodology and documentation practices aligned to the standards of international accounting bodies and industry best practices

A Snapshot of Our IT Risk Management Services

1 Cyber Risk and Security

- Cyber Risk Management
- Infra & App security assessments
- Enterprise security architecture review
- Secure SDLC review
- Identity & access management
- Cloud security and mobility security reviews

2 IT Governance and Compliance

- IT security policy & process review
- IT GRC (tools) review
- HITRUST, HIPAA, NIST, ISO alignment
- Data Governance
- GDPR & CCPA, SOX, SSAE16, PCI requirments

3 IT Risk Management

- ITRM framework design & rollout
- Third party InfoSec Reviews
- BCP & DR planning & implementation
- Software Asset Management

4 Forensic Investigation

- Evidence Acquisition
- Evidence Analysis
- Legal Documentation
- Forensic Data Reporting
- Legal Certification
- Court Depositions

5 Corporate fraud Prevention

- Know your Employees
- Company Data Protection Policy
- Review IT Security Policies
- Data Protection Process
- Data Governance
- Legal Framework

Mitigating Risk Across the Finance Sector

The internet is now the primary mechanism for financial transfers between banks and other institutions; most customers rely on online banking to manage their accounts and for the majority of point of sale payments. The more reliant on digital technology the financial system becomes, the more interconnected it is and the more vulnerable it is to cyber exploitation.

Consumers notoriously prefer convenience over security, and financial institutions encourage consumers to use online technology as a way of harnessing efficiencies and reducing operating costs. Malicious actors are not targeting the industry for mere financial gain: they are actively looking to exploit vulnerabilities that could be used to bring it down, thereby undermining confidence in the financial system and causing social chaos and turmoil to threaten the democratic way of life.

The financial industry's dense interconnectivities, broad digital footprint with consumers and extensive reliance on technological infrastructure expose it to a disproportionately large attack surface.

The financial industry experiences greater losses from cybercrime than any other sector, reportedly experiencing attacks three times as often as other industries.

The Threat Landscape for Finance Companies

To manage cyber risks appropriately organizations must set risk appetite, and drive focus on what matters. Our Cyber Risk Management framework starts by understanding who might attack, why, and how.

Who might attack?

- Cyber criminals
- Hactivists (agenda driven)
- State Sponsored hackers
- Insiders / partners
- Competitors
- Skilled individual hackers
- Rogue Organisations

What are they after, and what are the key business risks I need to mitigate?

- Theft of IP/strategic plans
- Reputation damage
- Business disruption
- Destruction of critical infrastructure
- Threats to health & safety
- Quick Profits

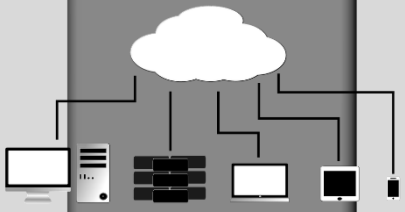
What tactics might they use?

- Spear phishing, drive by download, etc.
- Software or hardware vulnerabilities
- Third party compromise
- Multi-channel attacks
- Stolen credentials

What enables these attacks

Global Scale of Operations

Complex Interconnectivity

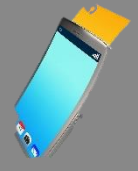


Systemic Significance

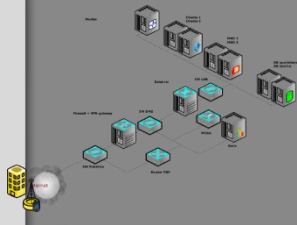
Contagion – Weak Links

Vendor Cyber Hygiene

Convenience Over Security



Widely Distributed Data



Impact of the Cyber Attacks

Contagion

- Global Interconnectivity
- Systems reaching beyond borders
- Weak links can be exploited
- Single Compromised node
- Has fast spreading effects

Disruption in Services

- WannaCry Attack of May 2017
- Distributed denial of service
- No transactions can be processed
- Critical Payments held

Cost of Consumer Losses

- Banks need to cover end user losses
- End user security Low
- Convenience over security
- Little incentive to follow security guidelines

Fraudulent Payment Orders

- Steal Credentials of Bank Staff
- Steal Credentials of Customers
- Allows account access - Phishing
- Fraud Transactions

Single Points of Failure

- Equifax financial data theft
- No clear alternatives
- Crises event SOP missing

Dark Web Data Publishing

- Finance Data highly in Demand
- Used by Governments
- Used by Rogue Organizations

Mutual Trust - Confidence Breached

- Following a Data Breach

Compliance in Financial Industry

- The *Reserve Bank of India (RBI)* published a circular, Digital Payment Security Controls, requiring regulated entities (REs) to establish a governance structure for digital payment products and services while implementing minimum IT security standards. Regulated entities include depository institutions and other financial organizations:
  1. Scheduled commercial banks (excluding regional rural banks)
  2. Small finance banks
  3. Payments banks
  4. Credit card issuing non-bank financial companies (NBFCs)

- *ISO/IEC 27001* is an internationally recognized standard
- for reducing security risks and protecting information systems.

- The *National Institute of Standards and Technology (NIST)* is the United State's equivalent of the (ISO) - an international organization governing national standards bodies.

- The *Sarbanes-Oxley (SOX)* act of 2002 is a law passed by U.S Congress to protect investors from financial scams. The SOX framework outlines best security practices for avoiding fraudulent financial transactions through a system of internal checks.

- *Payment Card Industry (PCI)* Data Security Standards (DSS) – is a set of standards for reducing credit card fraud and protecting the personal details of credit cardholders. The security controls of this regulation are designed to secure the three primary stages of the cardholder data lifecycle: Processing – Storage – Transfer. Every organization that processes customer credit card information must comply with PCI DSS, including merchants and payment solution providers.

Cyber Risk Case Studies

Sony Sambandh Case – Credit Card Theft

runs a website called www.sony-sambandh.com, targeting Non-Resident Indians.

Who

Impact

The company lodged a complaint about online cheating at the CBI which registered a case under Section 418, 419 and 420 of the Indian Penal Code. The matter was investigated, and Arif Azim was arrested. Investigations revealed that Arif Azim while working at a call centre in Noida gained access to the credit card number of an American national which he misused on the company's site.

What Happened

The website enables NRIs to send Sony products to their friends and relatives in India after they pay for it online and deliver the products to the concerned recipients. In May 2002, someone logged onto the website under the identity of Barbara Campa and ordered a Sony Colour Television set and a cordless headphone. She gave her credit card number for payment and requested the products to be delivered to Arif Azim in Noida. The payment was duly cleared by the credit card agency, and the transaction was processed. After following the relevant procedures of due diligence and checking, the company delivered the items to Arif. The company took digital photographs showing the delivery being accepted by Arif. The transaction closed at that, but after one and a half months the credit card agency informed the company that this was an unauthorized transaction as the real owner had denied having made the purchase.

In this matter, the CBI had evidence to prove their case, and so the accused admitted his guilt. The court convicted Arif Azim under Section 418, 419 and 420 of the Indian Penal Code - this being the first time that cybercrime has been convicted.

Cyber Risk Case Studies

Swift Money Transfer Case – Malware

SWIFT, has operated since 1973 as a junction for money transfers through messages between 11,000 financial institutions operating from approximately 200 countries around the world.

Who

Impact

On September 27, 2016 - four months after the initial report of fraud using SWIFT systems, SWIFT announced that it would activate a mandatory security standard for all of its customers. The framework of which organizations will be obligated to perform an annual self-assessment of compliance with security standards, and to report their findings to SWIFT as well as to the regulators in the relevant sectors

What Happened

In February 2016, it was published that approximately 81 million dollars was withdrawn from the Central Bank of Bangladesh using four fake transfers on SWIFT systems, “only a small” part of the approximately one billion dollars that the attackers intended to transfer for their use. the security company that investigated the incident, found that a sophisticated malicious code had been inserted into the banking system in Bangladesh that enabled the fake transfers and simultaneously “took care of” deleting alerts and records that leave traces so that bank employees had no indication of the transfers that were made. The money was transferred to a bank in the Philippines and from there the money was withdrawn in cash from casinos operating in the country.

The snowball of fraud incidents using SWIFT systems began to roll in April 2016 and since then it gained momentum, added more and more banks that fell victim to these schemes, and completely changed customers’ perception of the security level of the SWIFT systems and the components of the security level that they are supposed to provide to their customers, which affects confidence in the entire mechanism

Cyber Risk Case Studies

Cosmos Bank – Cyber Hacking Attack

Co-operative Bank Ltd., established in 1906, is one of the oldest Urban Co-operative Banks in India

Who

Impact

According to the cybercrime case study internationally, a total of 14,000 transactions were carried out, spanning across 28 countries using 450 cards. Nationally, 2,800 transactions using 400 cards were carried out.

What Happened

In August 2018, the Pune branch of Cosmos bank was drained of Rs 94 crores, in an extremely bold cyber attack. By hacking into the main server, the thieves were able to transfer the money to a bank in Hong Kong. Along with this, the hackers made their way into the ATM server, to gain details of various VISA and Rupay debit cards.

The switching system i.e. the link between the centralized system and the payment gateway was attacked, meaning neither the bank nor the account holders caught wind of the money being transferred.

This was one of its kinds, and in fact, the first malware attack that stopped all communication between the bank and the payment gateway.

Excelic Solutions for Cyber Safe Finance

- Humans are the weakest link in cybersecurity
- **End users**, from clinicians to billing and scheduling staff, as well as patients and caregivers who connect their personal devices with the hospital network, can unintentionally **threaten the cybersecurity** of the health facility
- Relevant and effective trainings,
- Data Leak Protection Solutions
- Defined Policies or **SOPs**
- Legal Binding with **NDA**
- Random **Forensic**
- **Endpoint Protection**

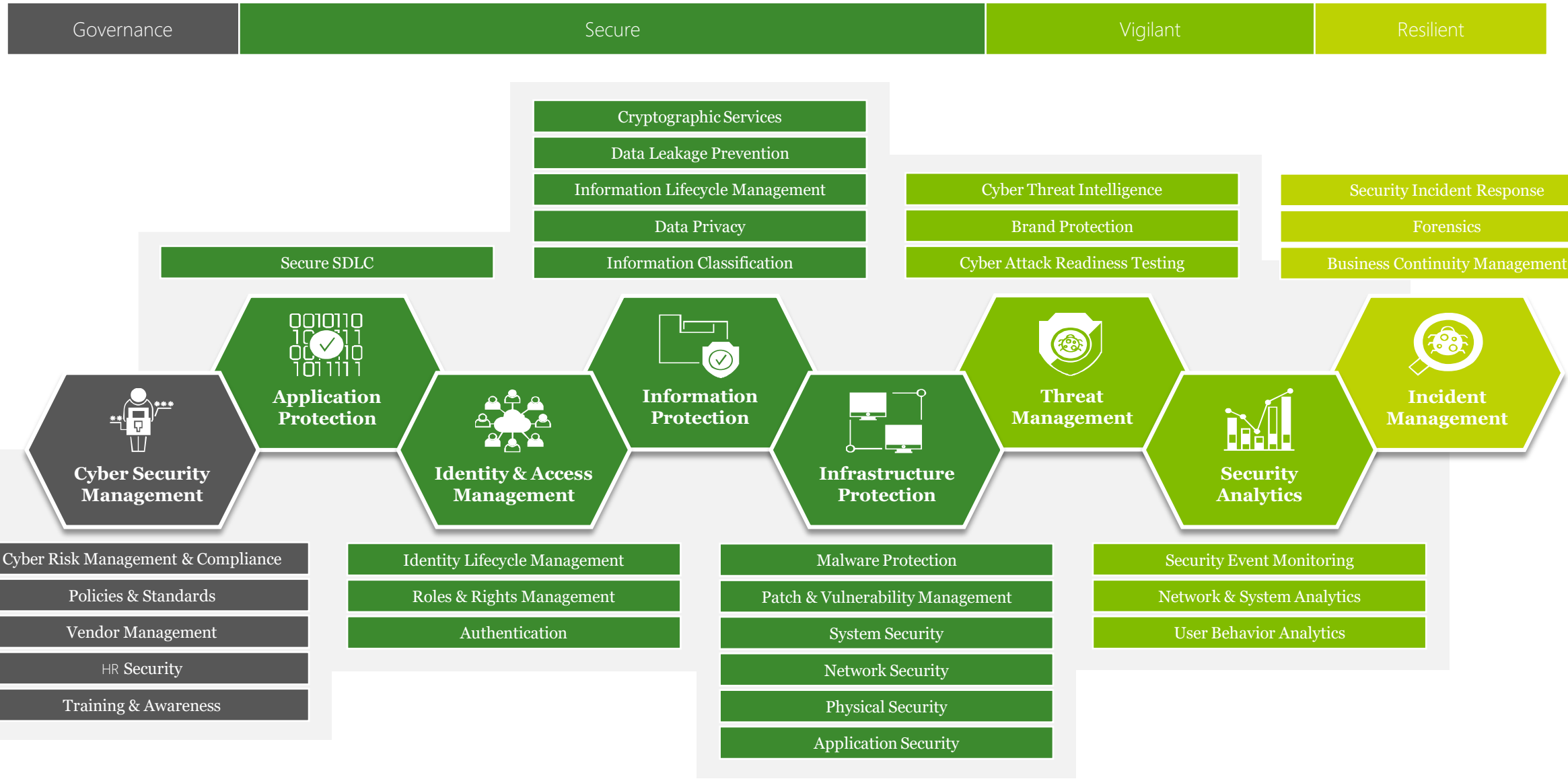
- Security Strategy and Framework
- Risk Assessment and VA/PT.
- Cloud Security
- Configuration Hardening
- Endpoint Protection Solutions.
- Administrative and other user privileges and SOPs

- NIST Compliance
- ISO 270001 compliance
- Security Audit.
- GDPR Compliance
- PCI Compliance

- **Centralized** visibility
- **Detect, Investigate and Respond** to critical company wide cybersecurity threats
- **Threat** Management
- Managed **Detection**
- Managed **Incident response**

- Rapidly detect cyber incidents
- Evaluate effectiveness of identified controls
- Remediate weakness in identified controls
- Independent testing and auditing functions

Excelic's Cyber Security Framework & Services



Corporate & Government Ties

TATA MOTORS
teltronic
ADITYA BIRLA GROUP
LARSEN & TOUBRO
Kawasaki
ALSTOM
mobility by nature
NSE
NSEIT
DAMM
Critical communication made easy
Edelweiss
Ideas create, values protect
CRRC
هيئة كهرباء ومياه الشارقة
Sharjah Electricity & Water Authority
GT20 CANADA
EURO T20 SLAM
SKF
LOVELY PROFESSIONAL UNIVERSITY
MANDATLY
Privacy Compliance Software
BCH
BOMBAY COFFEE HOUSE
BANDRA | FORT
destek
DhakDhak
India ke Dil ki Dhadkan
ARYANS
GROUP OF COLLEGES
D Y PATIL
UNIVERSITY
JBCN
International School
BKC
Your Growth Our Mission
RP
RAM PRIYANKA
Media Entertainments
KUAUSMEDIA
ENTERTAINMENT
FILM PRODUCTION, PR, CELEBRITY, EVENT & TALENT MANAGEMENT
Polaron
TECHNOLOGIES PVT. LTD.
LEGAL NEXTT

- Thank You