Cyber Security in FinTech Industry

1

Need and Importance of Cybersecurity

Technology has been evolving over the last few decades..

Late 80's

First ATM Launch in India

More than 2,00,000 ATMs in present scenario

Mid 90's

Internet was launched in India

More than 400 million users in present scenario

1998's

Internet Banking was launched in India

More than 45 million account users

Mid 2000's

IoT Foundation was established

More than 7 billion active IoT devices*

Mid 2000's

AWS Cloud Launched in India

More than 30% CAGR growth

Recent Years

Block chain implementations

Multiple use cases in the pipeline

Internet Of Things (IoT): Everyday physical devices getting computing capabilities and getting connected with the Internet in order to send, receive and process data. Thus, such devices can be controlled as well as monitored remotely due to its connectivity and processing power.

Amazon Web Services (AWS): Amazon offers cloud computing platform to businesses. It provides all three types of cloud services, namely, Software as a Service, Platform as a Service, and Infrastructure as a Service.

..and this evolution has resulted in more and more users connecting through the Cyber space Globally and in India

What happens in an Internet minute

Created by:
@Lori Lewis; @OfficiallyChadd

Global		India	
Internet users		***Internet users***	
3.4 billion	**3** billion	**478** million	**243** million
2017	*2015*	*2018*	*2014*
Connected things		***Smartphone users***	
8.4 billion	**6.3** billion	**456** million	**220** million
2017	*2015*	*2018*	*2014*

Digital channels

Digital business models

Digitization of business processes

Sources:
1. IAMAI report
2. Gartner
3. eMarketer

Customer Data

*Information provided intentionally **(explicit)**, or gathered **(implicit)** from available data streams*

. . . which has led to number of security incidents rising in India and globally. . .

FEB 18, 2016 @ 04:47 AM 20,456 VIEWS

The Little Black Book o

As Ransomware Crisis Explodes, Hollywood Hospital Coughs Up $17,000 In Bitcoin

Home » Airtel, Cyber Crime, Hathway, Internet, Internet Service Providers, ISP, Mobile

Internet in Mumbai slows down as DDoS attack clogs the network

By Vivek Pai on July 25, 2016

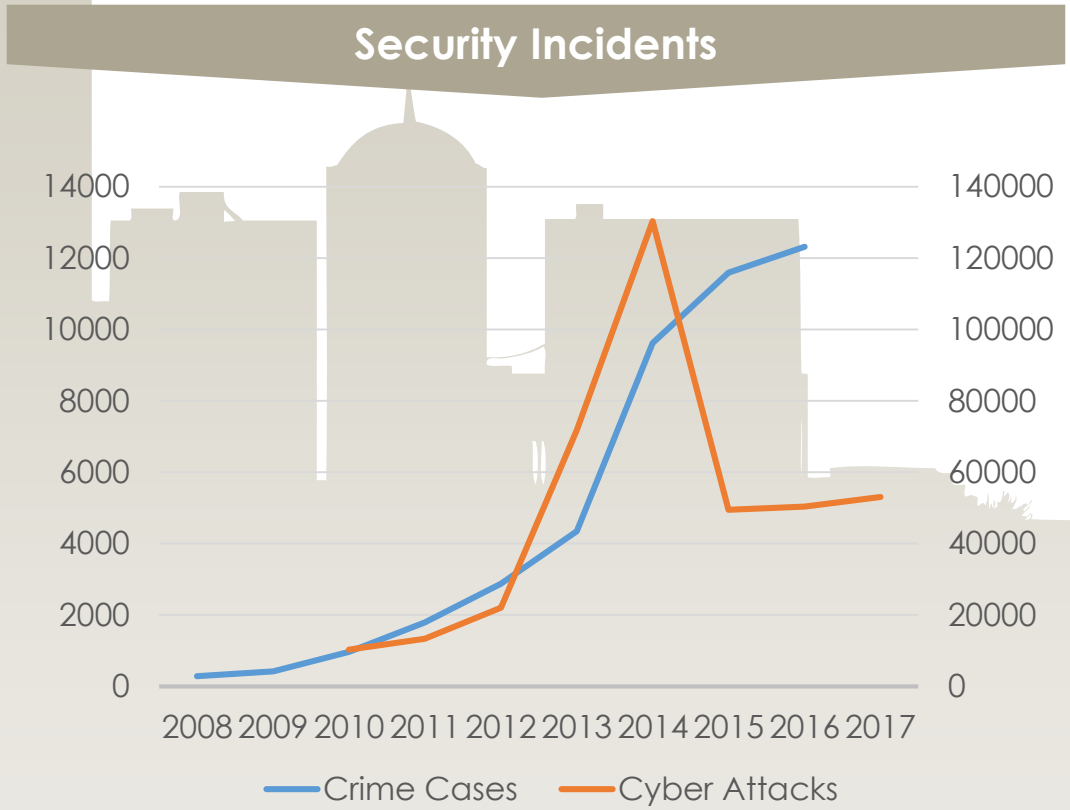
Philippines elections hack 'leaks voter data'

By Leisha Chi
BBC reporter

11 April 2016 | Technology Share

BlackEnergy Malware Used in Ukraine Power Grid Attacks

Posted: 01/13/2016 | By: CSIACAdmin | Leave a Comment



Source:
1. NCRB Crime Data
2. CERT-IN Security
3. Internet

2

Need for Cyber Security in FinTech

Why Cyber Security is important in the FinTech Industry ?

The FinTech industry has increased significantly in 2018 with more than $41 Billion raised

82%

82% of financial institutions expect to increase their partnerships with FinTech firms over the period 2017–22

71%

But this could be hampered by 71% of financial institutions viewing FinTech firms as a cyber security risk

Pen-Testing results of 21 of the Most Popular Trading Apps

95%

95% failed to detect rooted environments

67%

More than two-thirds stored sensitive data in log files unencrypted

62%

62% failed to implement SSL certificate validation

19%

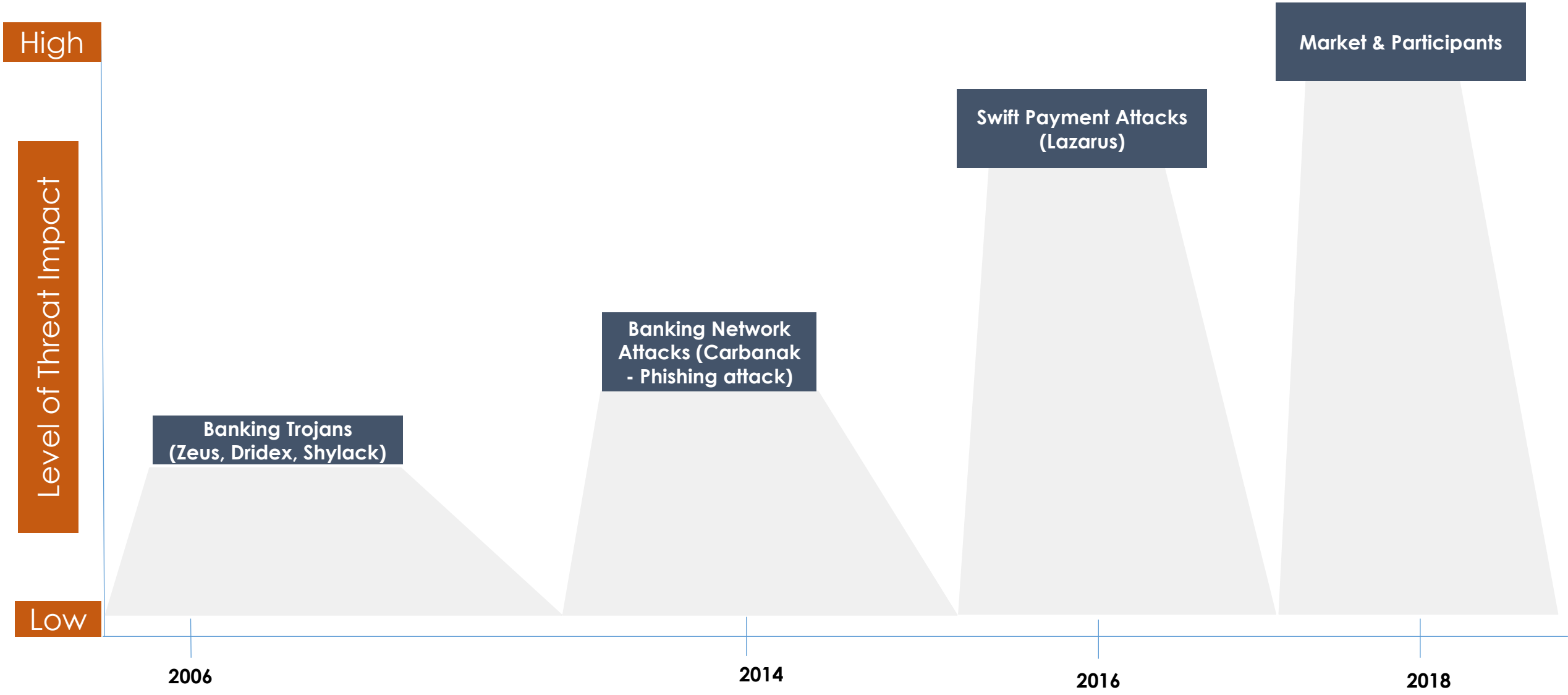
Almost 1 in 5 revealed the user's password in cleartext without cryptographic protection

Currently, only 32% of the FinTech companies priorities investment in their cyber security solution. Out of 2035 Fin tech startups in India, only 58 focus on Cybersecurity.

Source PricewaterhouseCoopers, Simmons & Simmons, IOActive

SSL certificate validation: Secure Sockets Later certificate is a file that is used to make the connection between browser (such as Chrome) and the server (on which the website is hosted) secure. By making the connection secure, it prevents the data(such as credit card details) to be stolen by hackers.

Evolution of Financial Threats



Recent Cyber Attacks on Financial Institutions

#	Institution	Year	Type of Attack	Details
1	Federal Reserve Bank of Cleveland	2010	Data Breach	Theft of 122,000 credit cards
2	Federal Reserve Bank of New York	2012	Data Breach	Theft of proprietary software code worth USD 9.5 Million
3	Sveriges Riksbank	2012	Business Disruption	Distributed Denial of Service (DDoS) attack left the website offline for 5 hours
4	Banco Central del Ecuador	2013	Fraud	13.3 Million USD stolen from the account of the city of Riobamba from the central bank
5	Federal Reserve Bank of Saint Louis	2013	Data Breach	Publication of credentials of 4,000 US bank executives by Anonymous
6	Central Bank of Swaziland	2014	Fraud	Theft of USD 688,000
7	ECB	2014	Data Breach	20,000 email addresses and contact information compromised
8	Norges Bank	2014	Business Disruption	DDoS attack on seven large financial institutions, resulting in suspended services during a day.
9	Central Bank of Azerbaijan	2015	Data breach	Theft of thousands of bank customers' information
10	Bangladesh Bank	2016	Fraud	The SWIFT credentials of the Bangladesh central bank were used to transfer USD 81 Million from its account at the FRBNY. Hackers tried to steal USD 951 Million.
11	Bank of Russia	2016	Fraud	21 Cyber-attacks aimed at stealing USD 50 Million from correspondent bank accounts at the central bank, resulted in a loss of USD 22 Million
12	Bank of Italy	2017	Data Breach	Hack of email accounts of two former executives

Source : IMF Working Paper : Cyber Risk for the Financial Sector

Key reasons for cyber threats in the FinTech Sector

1. **Understanding of Market practices :** *Some market practices which require trust, such as delivery free of payment and documentary collection,* ***potentially unsafe practices*** *including confirmations* ***via fax or email****, and the* ***long chain of interactions between unrelated Participants****, all provide a wide range of opportunities for* ***APT groups*** *to exploit.*

2. **Digitization/Automation:** *A general trend across all markets is the increasing desire to digitize and automate market operations for greater efficiency and to increase participation and revenue. This trend can be both positive and negative – it can lead to streamlined operations, greater speed and fewer errors* ***but only if designed and implemented to take into*** *account the cyber threat. People can also be lulled into a* ***false sense of security*** *and* ***trust*** *the machine which* ***cyber attackers will exploit.***

3. **Disruption and increasing Competition**: *The rise of FinTechs and other new entrants seeking to shake up markets is causing increased disruption. Whilst such change, innovation and competition is positive, it increases the* ***cyber risk as new entrants*** *and* ***incumbents*** *rapidly bring in* ***new technologies, services and ways of working*** *that are immature and* ***unable to withstand the increasing cyber threat.***

Recent Cyber Attacks on FinTech Firms

#	Institution	Year	Estimated Losses
1	Inputs.io	Oct, 2013	1.3 USD Million
2	GBL	Oct, 2013	5 USD Million
3	Bitcoin Internet Payment Services	Nov, 2013	1 USD Million
4	MT Gox	Jan, 2014	470 USD Million
5	BitPay	Dec, 2014	1.9 USD Million
6	EgoPay	Dec, 2014	1.1 USD Million
7	Bitstamp	Jan, 2015	5,3 USD Million
8	Bitfinex	May, 2015	0.3 USD Million
9	Gatecoin	May, 2016	2 USD Million
10	DAO Smart Contract	Jun. 2016	50 USD Million
11	Bitfinex	Aug, 2016	72.2 USD Million
12	CoinDash	July, 2017	7 USD Million
13	Tether	Nov. 2017	31 USD Million
14	NiceHash	Dec, 2017	64 USD Million
15	Coincheck	Jan, 2018	534 USD Million
16	Bitgrail	Feb, 2018	170 USD Million
17	Coinsecure	Apr, 2018	33 USD Million

Source :ORX News, Financial Times

3

Cyber Security in FinTech Markets

In the FinTech market, 4 types of financial markets need to be assessed to review and assess their vulnerability to APT groups

Foreign Exchange	The FX market is arguably the world's largest (by volume) and most liquid financial market and is vital to global trade and money flow.
Banking & Payments	The banking and payments market covers the fundamental movement of money between organizations and individuals and therefore underpins all other markets.
Trade Finance	Trade finance supports domestic and international trade transactions and as such is critical to facilitating global and domestic trade in goods.
Securities	Critical to the global economy, securities make up arguably the most complex and diverse financial markets, and include market areas such as trading equities, bonds and derivatives.

For each of the financial market, the threat & susceptibility factors shall be taken into consideration in order to assess the overall cyber threat.

Foreign Exchange Market

FX Market View

- The cyber risk scenarios would be focused on settlement infrastructures such as CLS and the interbank and retail level trading platforms.
- As the focal points in the FX market for transactions, the cyber risk would be to systems receiving and processing the FX orders and performing the netting calculations that determine the values of funds transferred. Malicious alterations to the orders and calculated values would affect the funds transferred and would be settled with finality.
- For trading platforms, the cyber risk is where there would be malicious alterations to the FX instructions received, thereby affecting the value of funds transferred in a trade.
- FX is the largest and most liquid financial market by volume. This means that potential financial gains would be very high if Market Infrastructures such as settlement institutions, common trading platforms and infrastructure – including SWIFT – were compromised.
- The forecasted cyber risk is therefore considered relatively low and is longer term when compared to other markets.

FX Participants View

- For Participants, the anticipated cyber risk is higher due to their larger numbers in the retail FX market. In addition, not only do they have varying cyber maturity, but there is also less regulation & oversight.
- Participants are particularly vulnerable to attacks on their business processes. This is where unstructured communications and data – such as email and instant messaging – are used for orders and confirmations, and where key information covering payment details and amounts could be altered.
- APT groups could also target systems used to generate the FX trade instructions to the market platforms to execute fraudulent transactions.
- Compared to the potential financial gain from FX Market Infrastructures, the gain from Participants would be more limited. This is due to the largely bilateral, lower margin trades which an attacker would need to manipulate in their favour, as well as the smaller amounts available from each participant.
- The forecast risk to FX participants is much higher when compared to FX Market Infrastructures. Overall the risk is considered less than other Market Infrastructures & Participants, there by the risk is medium.

Banking & Payments

Market Infra

- The infrastructures such as RTGS, Retail Payment Systems, SWIFT, are said to be critical and the cyber threat is said to be managed.
- For RTGS, the threat from APT groups is primarily focused on altering the ledger of settlement accounts maintained for RTGS Participants.
- For RPS, the cyber risk could target modification or falsification of individual payment instructions or the netting or authorisation mechanisms for payments to benefit the attacker
- Attacks on Market Infrastructures would be very lucrative as they would be attacking the direct movement of money, but cashing out the gain would be more difficult as further breaches elsewhere would be required.
- Successful attacks on SWIFT, RTGS, and RPS payment
- systems would yield high gains as they control the flow of money.
- Overall, considering the threat and susceptibility factors, the cyber risk to Market Infrastructures within banking and payments is relatively low and is considered a longer term risk.

Participants View

- For Participants such as banks, corporates, governments and individuals, there is a lower chance of detection when compared to the Market Infrastructure level.
- The increased investment from larger financial institutions on cyber security is displacing attacks and attackers "to target new geographies, individual and enterprises who do not have similar levels of protection.
- APT groups could also target systems used to generate the FX trade instructions to the market platforms to execute fraudulent transactions.
- The overall cyber risk to Participants, particularly for those with less investment and maturity in cyber security, is considerably higher and more near term than for the Market Infrastructure.
- Attacks on Participants can yield US$ millions for the attackers, as evidenced by the ongoing attacks on SWIFT members..

Trade Finance

Market Infra

- An area that APT groups would potentially target is documentary collection and documentary credit – in both Market Infrastructures and Participants.
- Hackers also rely on documents, often physical papers, being the evidence to release goods or funds, and complex interactions – such as those between importers, exporters, their respective banks, customs and transport agents – are common.
- The combination of little standardisation and the widespread use of emails, spreadsheets and word processors, means that it is relatively simple for APT groups to gain access either to Participants or trade finance provider IT infrastructures and modify these documents.
- Manipulating key information on the Blockchain, such as payment beneficiary details and confirmations, and then simply waiting for the automated self-executing aspects to deliver the assets to the attacker.
- Subverting or creating false nodes to manipulate the consensus decision process that underpins the Blockchain – thereby enabling the attacker to determine the outcome, such as approving payments, confirming conditions met or releasing of assets.
- A potentially higher reward is on offer from attacks on Market Infrastructure as they would be handling multiple trade finance transactions for multiple Participants. However, such attacks and cash outs are more complex than those on Participants.
- The cyber risk is considered to be medium term.

Participants View

- At the Participant level, the inherent lack of standardisation and structure in processes and documentation and the reliance on unstructured and unverified communications combined with the higher numbers of Participants of differing cyber maturity levels, provides a wide field of opportunities for APT groups to take advantage of.
- The exploitation of unstructured data – such as word processing documents and spreadsheets and modifying critical information such as payment details and terms to benefit the attacker – is a particularly important area of weakness.

Securities Market

Market Infra

- Manipulating data held in the infrastructure itself, such as securities ownership in Central Securities Depositories (CSD) and values, beneficiaries of trade transactions in Central Counterparties (CPP) and Electronic Trade Confirmation (ETCs).
- Manipulating market and reference data such as Standing Settlement Instructions (SSIs) and pricing in information service providers that are relied on to enable fraudulent payments, relaying incorrect material financial information to influence share pricing or exploiting algorithmic trading through fake orders (market manipulation).
- Attacking the mechanisms which match trades and calculate settlement values to fraudulently increase the gain on trades to the attackers benefit.

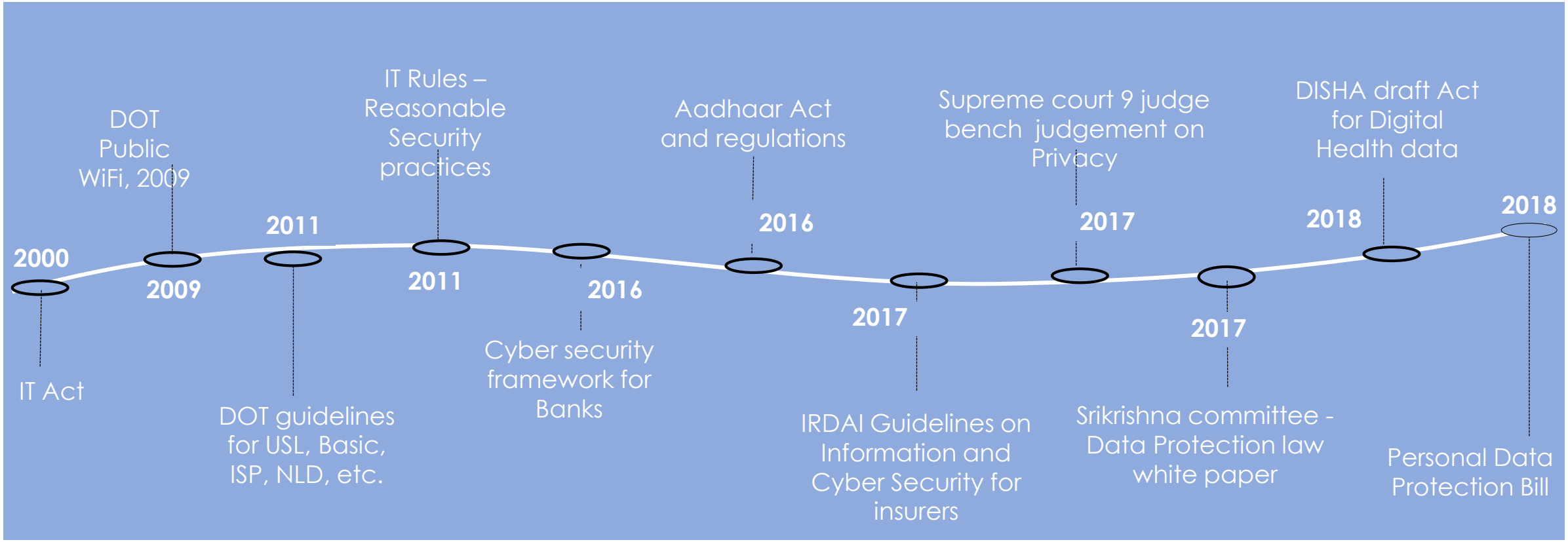
Participants View

- Falsifying trade orders and exploiting unstructured communications and data such as email and faxes used for orders, changes and confirmations.
- Exploiting market practices, including "delivery free of payment" to steal securities.
- Falsifying instructions to Market Infrastructures such as CSD, requiring changes in securities ownership or changing SSIs at reference data providers.

4

Cyber Security Regulations

Security and Privacy Laws and Regulations in India have evolved over a period of time. . . And are being continuously strengthened



India has also defined guidelines with respect to protecting the data and information of the citizens, thereby strengthening the laws around Privacy

01
Overall

Information Technology Act (IT Act), 2000, and section 43A of IT Act

- Laid the foundation of data privacy and data protection
- Reasonable Security Practices and Procedures and Sensitive Personal Data or Information
- Section 72-A

02
Overall

Srikrishna Committee – the Draft Data (Privacy and Protection) Bill, 2017

- 'Ensure growth of the digital economy while keeping personal data of citizens secure and protected'
- Proposed framework paves the way for a robust privacy regime

03
Sectoral

Digital Information Security in Healthcare Act (DISHA)

- Regulate the generation, collection, storage, transmission, access and use of all digital health data (DHD)
- Draft stage for public consultation

Regulators across various sectors have been pushing organizations to ensure security and privacy of their operations

Business enabling technology is fast evolving

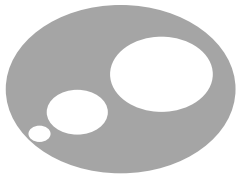
The threat landscape has become complex

There is a need for a forward looking cyber security framework

Cyber aware board & Strong Governance

Building cyber resilience

Customer protection



Focus on extended ecosystem

24 x 7 Monitoring with advanced real time capabilities

Cyber intelligence and collaboration

5

Understanding Cyber Security

Common Cyber Security related definitions. . .

Confidentiality	Ensuring that information is neither made available nor disclosed to unauthorized individuals, entities, processes or systems;
Integrity	Guarding against improper information modification or destruction;
Availability	Ensuring that information is accessible and usable by authorized users/ entities;
Authenticity	Establishing confidence that information is valid, verified, and can be trusted;
Non-Repudiation	Able to prove or establish the occurrence of a claimed event or action and its originating entities;
Identification	Initiating a process to identify an entity and to verify its professed identity;
Authorization	Approving an information system's operations based on a documented set of security controls and an authorization matrix; and
Accountability	Ensuring that the actions of a user/ an entity is traced uniquely to that user/entity

Classification of Information …..

- **Confidentiality**

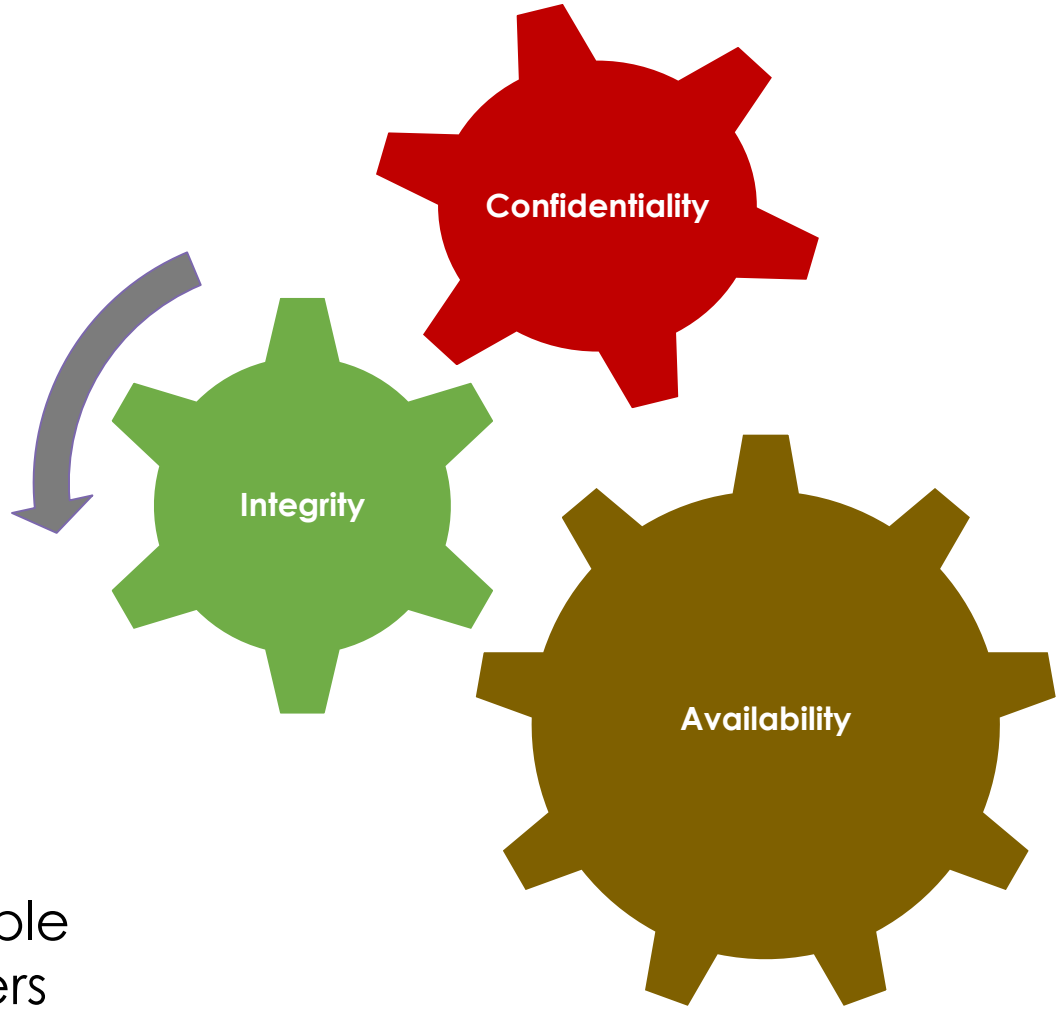
  Prevent sensitive information from being disclosed to unauthorized recipients

- **Integrity**

  Ensure maintenance of consistency, accuracy and trustworthiness of information

- **Availability**

  Ensure that information is available when required to authorized users



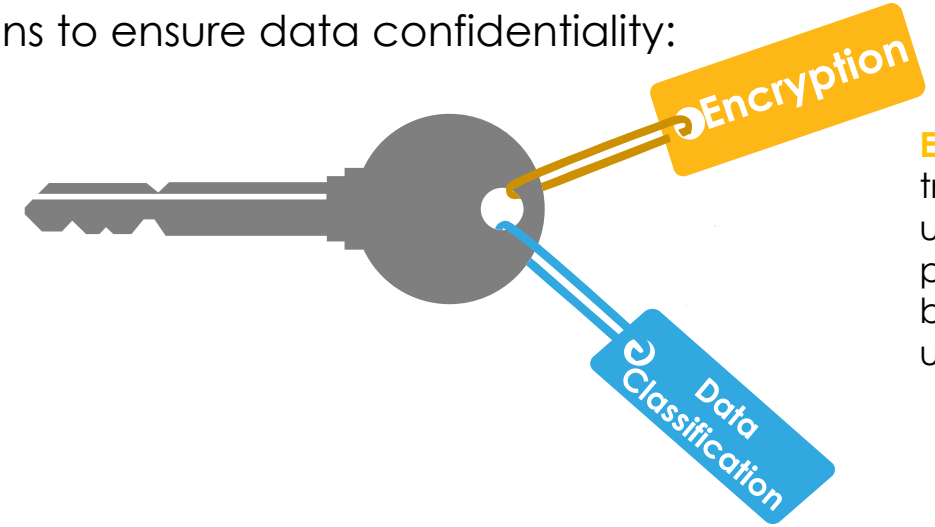
Data Confidentiality

Data Confidentiality is about protecting data against unintentional, unlawful, or unauthorized access, disclosure, or theft.

Consider the following when managing data confidentiality:

1. To whom data can be disclosed
2. Whether laws, regulations, or contracts require data to remain confidential
3. Whether data may only be used or released under certain conditions
4. Whether data is sensitive by nature and would have a negative impact if disclosed
5. Whether data would be valuable to those who aren't permitted to have it (e.g., hackers)

Security solutions to ensure data confidentiality:



Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text

Data Integrity

Data integrity refers to the fact that data must be reliable and accurate over its entire lifecycle. Uncorrupted data (integrity) is considered to be whole and then stay unchanged relative to that complete state.

Consider the following when managing data integrity:

1. Whether data must remain accurate and uncorrupted
2. Whether data must be modified only by certain people or under certain conditions
3. Whether data must come only from specific, trusted sources

Minimize Data Integrity risks by ensuring the following:

- Follow a software development lifecycle (SDLC)
- Validate your computer systems
- Implement audit trails
- Implement error detection software
- Secure your records with limited system access
- Maintain backup and recovery procedures
- Design a Quality Management System with SOPs and logical controls
- Protect the physical and logical security of systems
- Properly train users and maintain training records

Useful Security Solutions:

6

Cyber Attacks and its Impact

Anatomy of a Cyber Attack

WHAT will happen ?

- **Data leakage**
- **Service disruption**
- **Change in payment instructions**

WHERE it starts ?

- At **home, office or on the move**
- **Laptop / Desktop / Mobile**
- Servers and applications in a **data center**

WHY will attacker attack you ?

- **Money** (ransom-ware or data that can be sold)
- Just for fun or challenge
- Hired by **Competitors**

HOW it happens ?

- A **broken process**
- P**hishing email**
- A **targeted technology attack**
- Done with lot of preparation and understanding

WHO will do that ?

- Third party contractor/distributor
- D**isgruntled employee**
- **Competitors**/Corporate espionage
- Somebody with **state or corporate funding**

Anyone can be and is being attacked - 6.2 lakh new viruses every day!!
Be ready to timely detect, quickly respond and comprehensively resolve

Potential threats & Impact of security breaches

Who Could be Potential Intruders?

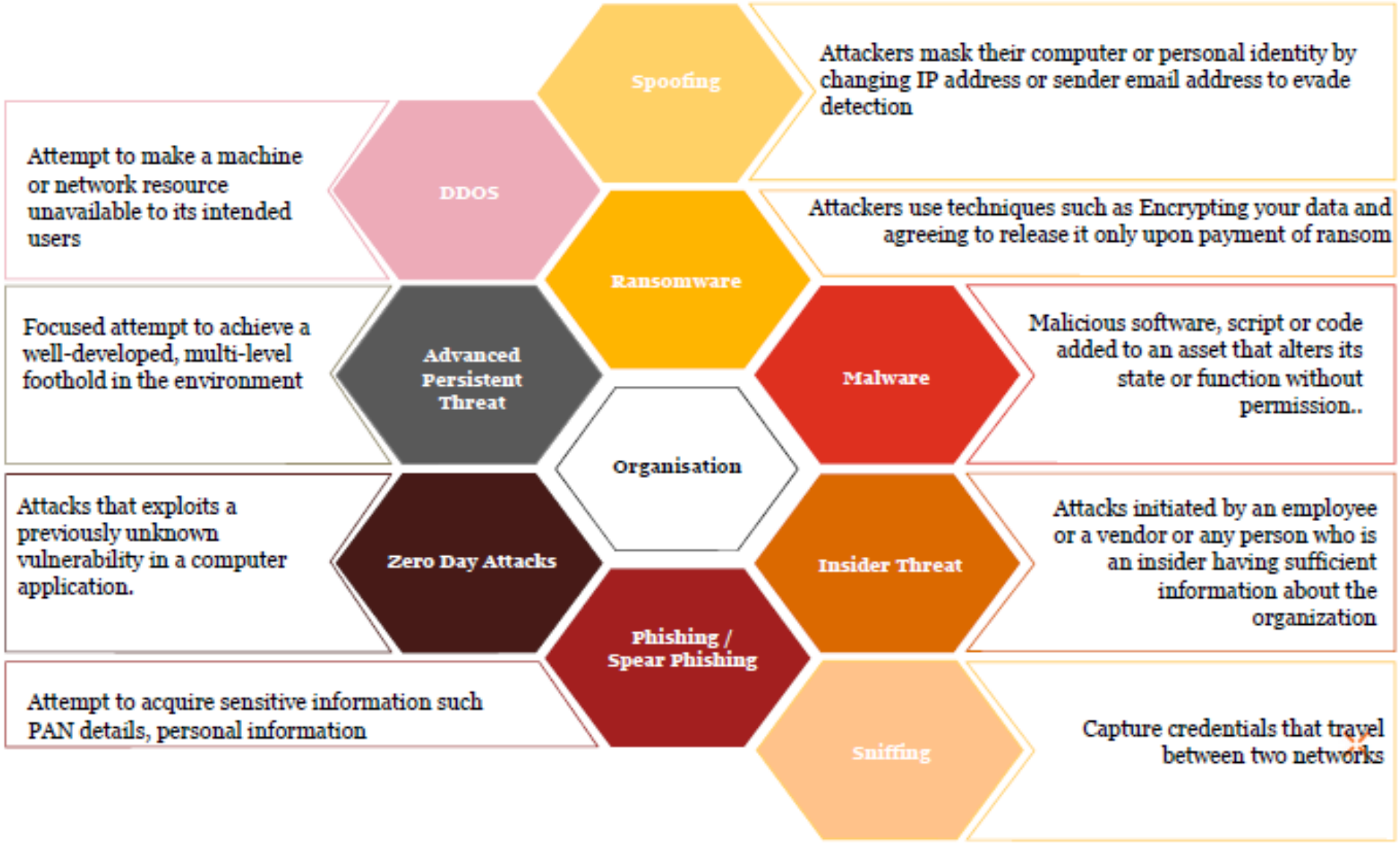
Business Competitor

Disgruntled staff or ex-employees

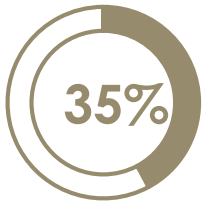
Hacktivists

Cyber Criminals

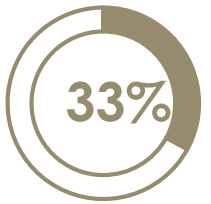
Common Cyber Threats faced



Disruption of Business Processes



Theft of intellectual property/sensitive data



Reputational damage

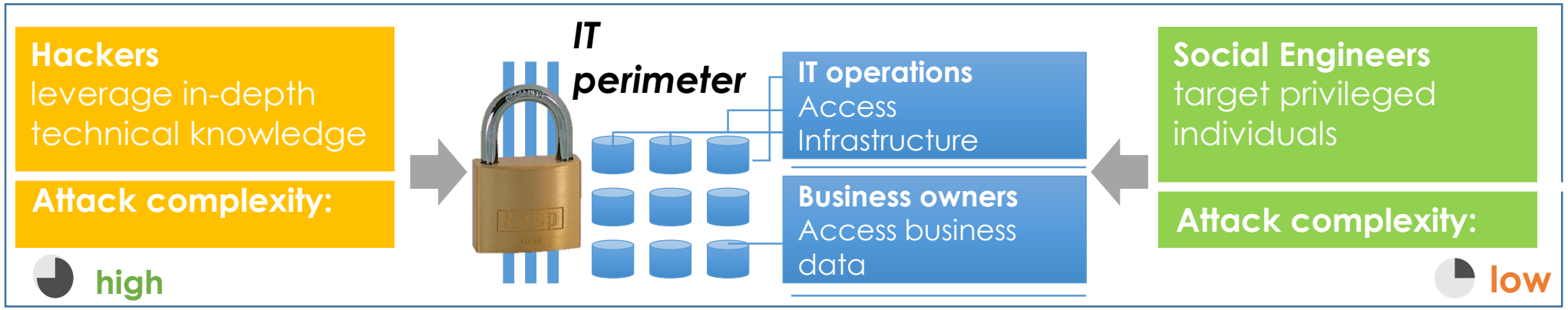
Financial loss

Employee moral

Regulatory non-compliance

Cyber Threat: Social Engineering

- **Social Engineering** is an often overlooked but regularly exploited threat; Exploiting "human factors" to bypass Information security restrictions.



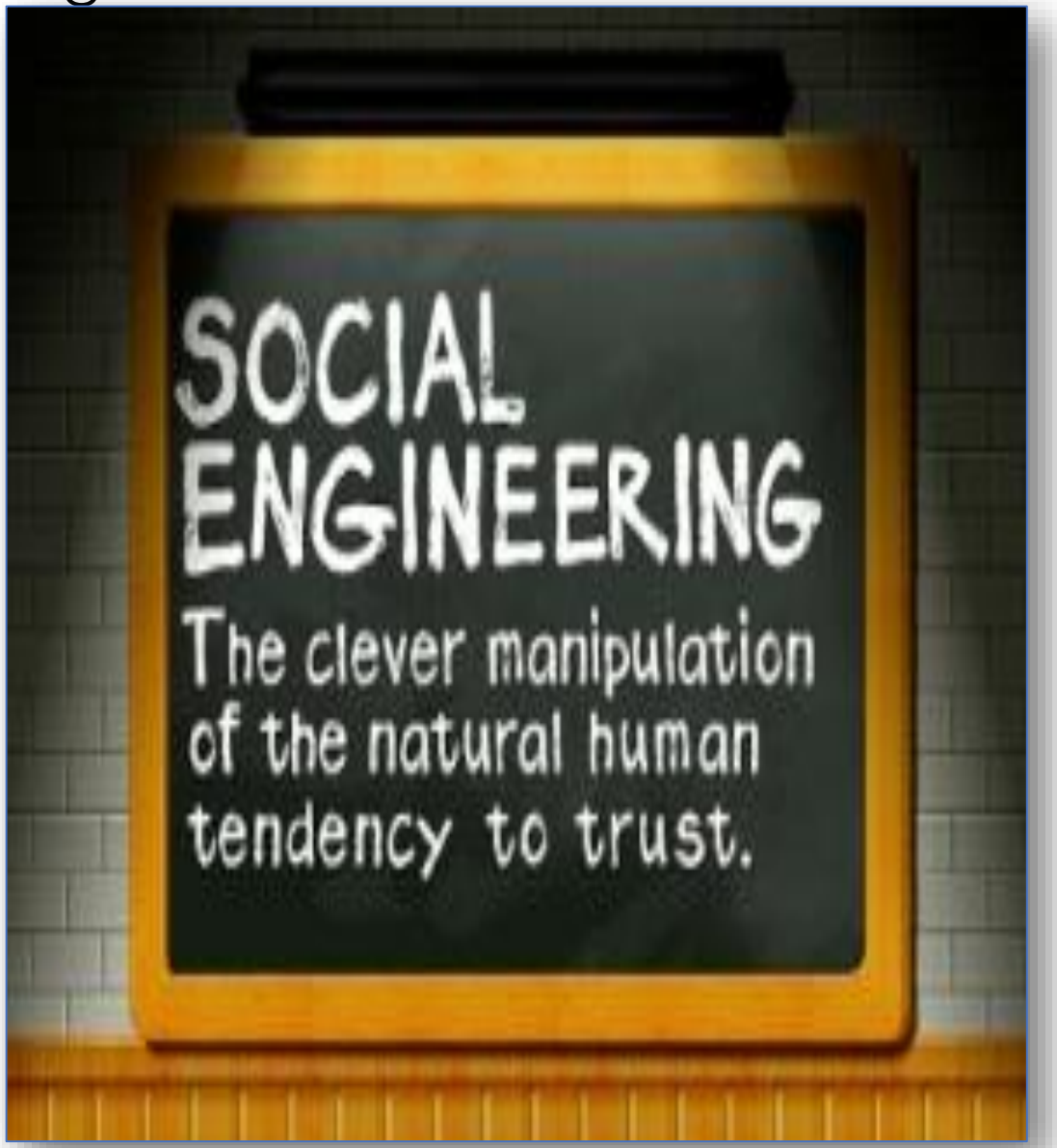
- **Impersonation:** Social engineers often impersonate authorities.
- **Manipulation:** Social engineers try to lure their victims into voluntarily circumventing security restrictions.
- **Exploitation of helpfulness:** People like to be helpful and supportive – Social engineers exploit this fact.

Social Engineering– Control Measures

Do not reveal sensitive information while on a telephonic conversation, on voicemail or on answering machines

When asked for potentially confidential data by someone you don't recognize, always ask to see their identification

Watch out for 'shoulder surfers' - people who may be reading confidential information on your computer screen



Cyber Threat: Phishing

Phishing refers to use of deceptive computer-based means to trick individuals into disclosing sensitive personal information

What to look for in a phishing email…

Even if a link has a name you recognize somewhere in it, it doesn't mean it links to the real organization. Roll your mouse over the link and see if it matches what appears in the email. If there is a discrepancy, don't click on the link. Also, websites where it is safe to enter personal information begin with "https" — the "s" stands for secure. If you don't see "https" do not proceed.

Forged link

The point of sending phishing email is to trick you into providing your personal information.
If you receive an email requesting your personal information, it is probably a phishing attempt

Requests personal information

Internet criminals want you to provide your personal information now. They do this by making you think something has happened that requires you to act fast. The faster they get your information,
the faster they can move on to another victim

Logo Design

Phishing – Control Measures

Legitimate organizations and services should never ask for sensitive information via email. They have it on record already

Don't reveal any passwords, personal information, financial credentials or organizational information without verifying the source

If you are asked to visit a website, just open a browser and type in the already known address

Legitimate online services will never threaten to lock your account immediately or scare you with shocking transaction details

Replying to phishing emails may expose private info or even IT vulnerabilities

Cyber Threat: Vishing

Vishing is a form of voice over internet protocol (VoIP) phishing attack where a caller uses social engineering via a phone call to convince a victim to provide the victim's sensitive information

Methods of Operation:

Voice call can either be real-time or recorded

In case of a recorded call, if answered by the potential victim, the recorded voice message is played to warn the victim that malicious activity has been performed on his/her account and personal bank account details are needed for verification purposes

Once the victim provides these details, the Visher may use them for fraudulent transactions.

Vishing - Implications

Step 1

- Fake caller identified himself as an employee from a bank.
- Informs the user that his debit card would be blocked if it was not updated immediately.

Step 2

- Asks for basic questions like name, age and his debit card PIN. Informs that the call is under security protocol.
- On receiving the pin Rs. 63,000 is withdrawn from the user's account.

Step 3

- The SIM card is removed or destroyed
- Another one is used for the next crime.

Another example of a vishing call is as follows: A conman pretending to be a Senior in your organization and asking you to send critical and sensitive information related to your firm and threating for taking serious actions if not done so

Cyber Threat: Smishing

Smishing is a form of criminal activity using cell phone text messages to deliver bait to induce people to divulge their personal information. The method used to actually capture people's information in the text message may be a website URL

Methods of Operation:

SMS can either be instant or forwarded

The potential victim receives an SMS, it contains information to warn the victim that malicious activity has been performed on his/her account and personal bank account details are needed for verification purposes or the victim is asked for his/her password masking a senior's identity

Once the victim provides these details, the Smisher may use them for fraudulent transactions

Smishing - Implications

Step 1

- A conmen duo messaged random numbers, asking people interested in earning Rs.10,000 per month to contact them
- They claimed to be working with a US-based advertising company which wanted to market its client's products through SMS

Step 2

- 10 SMS's were sent to the registered subscribers and were promised handsome commissions if they managed to rope in more subscribers by forwarding the SMS's
- The duo invited people to become agents for the scheme

Step 3

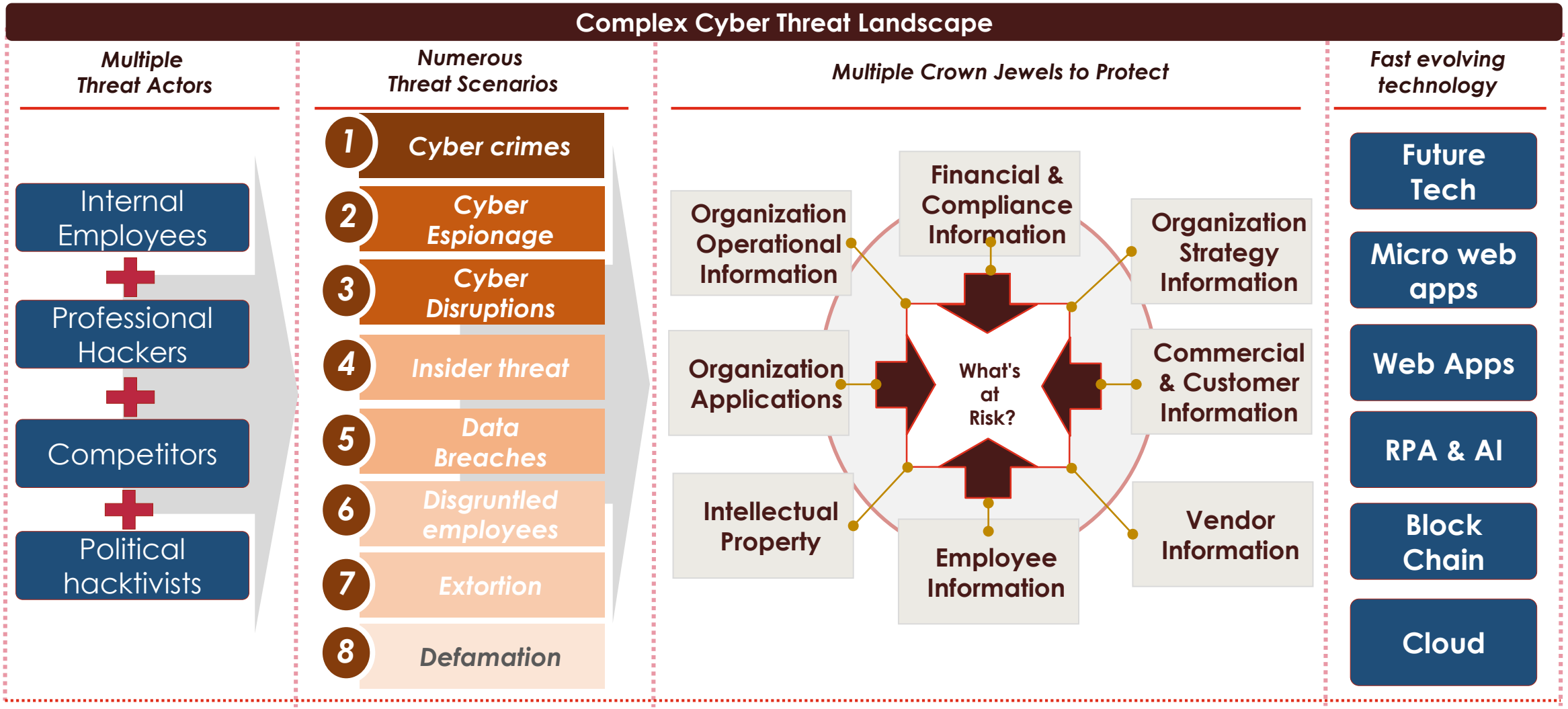
- The duo paid up small amounts. But when cheques and pay orders of larger sums issued by the duo were not honored, the agents got worried.
- The SMSs too suddenly stopped.

Variations: Another example of smishing: A fraudster sending an SMS announcing you as a winner of prize money from some international organization and asking you to send your PII along with your bank account details /employee details to claim the prize

7

Cyber Security for Organizations

Firms should recognize the entire threat landscape and accordingly formulate the strategy



How FinTech companies should be well prepared for Cyber Security Risk

Industry- and sector-aligned solutions

Align with the business

Prioritize investments, allocate resources, and align security capabilities with the strategic imperatives and initiatives of the organization.

Adapt to the future

Assess the opportunities and security-related risks of new technology adoption and dynamically changing business models.

Manage risk and regulations

Efficiently and effectively identify, evaluate, and manage risk to the business while addressing the evolving regulatory requirements.

Anticipate and respond to security crises

Plan, detect, investigate, and react timely and thoroughly to security incidents, breaches, and compromises.

Secure by design

Create sustainable security solutions to provide foundational capabilities and operational discipline.

Address threats and weaknesses

Anticipate changes in the risk landscape through situational awareness of the internal and external factors impacting the business ecosystem.

Enable secure access

Provide integrated and secure processes, services, and infrastructure to enable appropriate controls over access to critical systems and assets.

Safeguard critical assets

Identify, prioritize, and protect sensitive or high-value business assets.

Business-led approach – diverse capabilities

Every FinTech firm should devise a cyber security strategy keeping in mind the security lifecycle

- Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities
- Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services
- Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
- Develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event

Relevant Security Standards to build the cyber security framework which every FinTech organization should consider ……

1	**Security Standards**	*ISO 27001:2013* Information Security	*ISO 22301:2012* Business Continuity	*ISO 31000:2009* Risk Management
2	**International Standards/ Regulations**	NIST CSF NIST SP 800-53	PCI-DSS	HIPPA
3	**Policies and Guidelines in India**	Information Technology Act, 2000	National Cyber Security Policy	National Information Security Policy, MHA
4	**Cyber Security Bodies in India**	National Cyber Coordination Centre (NCCC)	National Critical Information Infrastructure Protection Centre (NCIIPC)	CERT-In State CERTs Sectoral CERTs

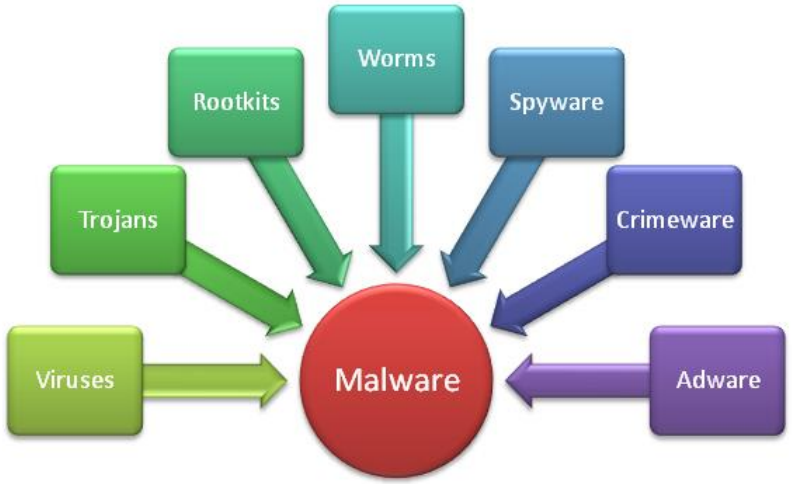
Keys factors for success in Standards implementation

1. ***Management Commitment – Top Down Approach***
2. ***Well defined roles and responsibilities***
3. ***Budget and resources***
4. ***Understanding of the organisations processes and the critical control points***
5. ***Training and support***
6. ***Alignment of business goals and standards objectives***
7. ***Continuous monitoring cycle***
8. ***Monitor and Remediate non-compliance***
9. ***Maintaining documentation***

8

Cyber Security for Individuals

Malware – Definition and prevention



Malware is any code or program which can execute an unintended or harmful purpose to the host's system.

The purpose can be stealing information, interrupting processes, spying the host, forced advertising, and so forth.

Make sure that you have the anti-virus software installed with the latest update

Never try to Bypass/ disable your virus scanning feature (scanning engine). They're there for a reason!

Do not click on any unidentified links in your email

Do not attempt to install third party utilities, including freeware

Virus – Implications

Viruses can corrupt and damage your data

Viruses can make your equipment malfunction

Viruses can destroy entire computer systems, rendering them inoperable

Virus can result in a huge security breach resulting in financial loss

Virus can give freeway access to adversaries to operate your systems

Virus can originate from infected Diskettes or other removable media

Free or 'questionable' software is often a potential source of virus

Files downloaded from the Internet may contain viruses

Email attachments can carry viruses

Laptop/Desktop Security - Implications

Step 1

He is watching You

- Victim leaves the laptop/desktop unlocked and unattended.
- Hacker grabs the opportunity to steal organizational information and misuse the laptop/desktop.

Step 2

Confidential

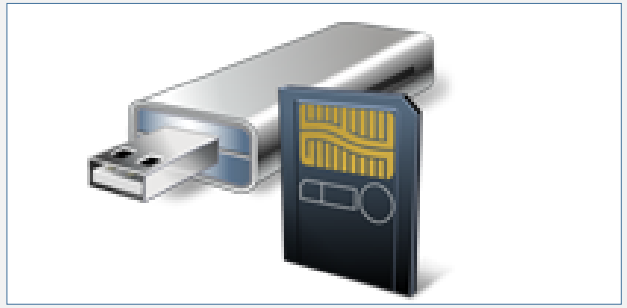
- Organizational/sensitive information is being stolen and misused by the Hacker
- Hacker will share the information which will lead to a corporate espionage or change the password of the laptop/desktop

Step 3

- Victim is held responsible for the loss of data and has to deal with the consequences.
- As a result the organization is directly impacted due to loss of critical information.

USB drop Awareness - Implications

1. Infected USB Dropped



- Hacker plans to steal organizational information through infected USBs
- Hacker drops and scatters malware infected USB mass storage devices in the office premises

2. USB Plugged in System

- Victim spots the USB and picks it up to check the information on the storage device
- Victim plugs in the USB Mass storage device into his/her system

3. System Hacked

- Victim's computer is infected with virus as soon as the USB is plugged in
- As a result sensitive information needed from the system is stolen by the hacker

Another example of a USB Drop incident is as follows : A colleague shares his/her USB with you. After plugging in you realize that the device was infected with virus. All your sensitive organizational information is compromised.

Internet Security

Being Internet Security Aware means you understand that there are people actively trying to steal data that is stored within your organization's computers. That is why it is important to protect the assets of the organization and stop that from happening.

 Websites	Controlling unauthorized use of the Internet and restricting the access to: a) Any site containing offensive material; b) Terrorism related websites; c) Sites distributing illegal goods, software, hacking tools and pirated material;
 Utilization	Restrictions on popular websites of non business nature which may lead to high utilization of bandwidth and restrict legitimate business use of the available bandwidth;
 Public Forums	Restriction on forums which allow users to engage in personal discussions, posting of personal profiles, engaging in any kind of trading / eCommerce, auctions etc..;
 Proxy	Under no circumstances, should you ever try to bypass the restrictions imposed by the proxy.

Mobile Security

Security Concerns

1

Information Security

Exposure of critical information

A wireless intruder could expose critical information

2

Lost or Stolen devices

A lost or stolen device can lead to entire corporate intranet being threatened

3

Mobile Viruses

Mobile viruses can take advantage of security holes in applications

4

Bluejacking

Bluejacking

Sending nameless, unwanted messages to other users with Bluetooth-enabled Mobile devices

5

Bluesnarfing

Bluesnarfing

Bluesnarfing is the theft of data from a Bluetooth phone

6

Malicious software and viruses

Worms disturb the phone network by spreading from one mobile to other through Bluetooth, Infrared or MMS

Email Security

Think before you click send!!

Improper use of email by users can lead to unauthorized information disclosure and could bring the organization to disrepute

Of the 247 Billion email messages sent every day, 81% are pure spam.

Password Security

How to create a strong password

Passwords should have minimum length of 8 characters

Passwords should not contain: your name, NetID, dictionary words, or predictable patterns

Passwords must include the following: combination of alphabets, numbers and special characters (*, %, @, #, $, ^)

Passwords should be changed every 45 days

Last six passwords should not be used

Few examples of strong passwords
Ttl*h1wwyr - Twinkle Twinkle Little Star How I Wonder What You Are

Safe Computing – Laptop/Desktop Security

- **Laptop and Desktop is one of the most critical assets in Galaxy. It contains all your confidential information which has to be protected from falling into the wrong hands.**
- **A minor distraction is all it takes for a laptop /desktop security breach to take place. All the valuable information stored on it may get accessed by unauthorized users**

Do's and Don'ts :

1. Do not change any hardware configuration, settings in operating system or any applications installed on desktops.
2. Do not connect modems to the machines unless and otherwise approved by the IT helpdesk
3. To prevent unauthorized access while desktop is unattended for short duration, locked the system with password protection
4. Log out of all applications or turn off the desktop when leaving the desktop unattended for extended period of time
5. Do not enable sharing of folders in your Desktop with other users over the network
6. Take adequate measures for physical protection of laptop
7. Do not share folders or disk drives in individual PC's or laptops unless share level access controls have been enabled

Clean Desk Policy

A clean desk policy states that it should be ensured that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation

• Ensure that your screen is locked, whenever you leave your workstation by using 'Ctrl' + 'Alt' + 'Del'+'Enter' or 'Windows Key + L'	• Do not let anyone else use your laptop
• Keep filing cabinets shut and locked, when unattended	• Do not leave any documents/files containing confidential information unattended
• Documents containing sensitive data should be shredded before disposal	• Do not leave photocopiers, fax machines and other office equipment unattended and ensure they are cleared of papers and any storage media
• Keep confidential information in secure storage	• Do not stick you passwords as a note on your laptop

Thank you