



INFORMATION ETHICS, PRIVACY & CYBER SECURITY IN SUPPLY CHAIN

R U N N A R I N S I W A P I M O N

SESSION OVERVIEW

01

Ethics in information technology

Overviews of ethics in business & IT users

02

Information privacy

How IT affects privacy rights & current privacy issues

03

Information security

Information security threats in supply chain context

04

Risk management & mitigations

Approaches to handle information privacy & security



ETHICS IN BUSINESS WORLD

The ethical & privacy issues are closely related, and both raise significant questions involving access to information in the digital age.

Delicate balance between accessing to information and the appropriate use of information is best maintained by **ethical** employees who conform to the organization's **code of ethics**.

Ethics refer to the principles of right & wrong behaviours within a society.

A Code of Ethics is a collection of principle that are intended to guide decision making by members of an organization.





ETHICAL CORPORATE FRAMEWORKS

Utilitarian approach

The ethical corporate actions should produce the greatest good and does the least harm for all affected parties

Rights approach

The ethical corporate actions should best protect and respect the moral rights of the affected parties

Fairness approach

The ethical corporate actions should treat all human beings fairly based on some defensible standard

Common good approach

Respect and compassion for all others are the basis for ethical actions

Deontology approach

The morality is a duty, based on whether that action itself is right or wrong under a series of rules or compliance, rather than based on the consequences of that action

FUNDAMENTAL TENETS OF ETHICS

Fundamental tenets of ethics include:

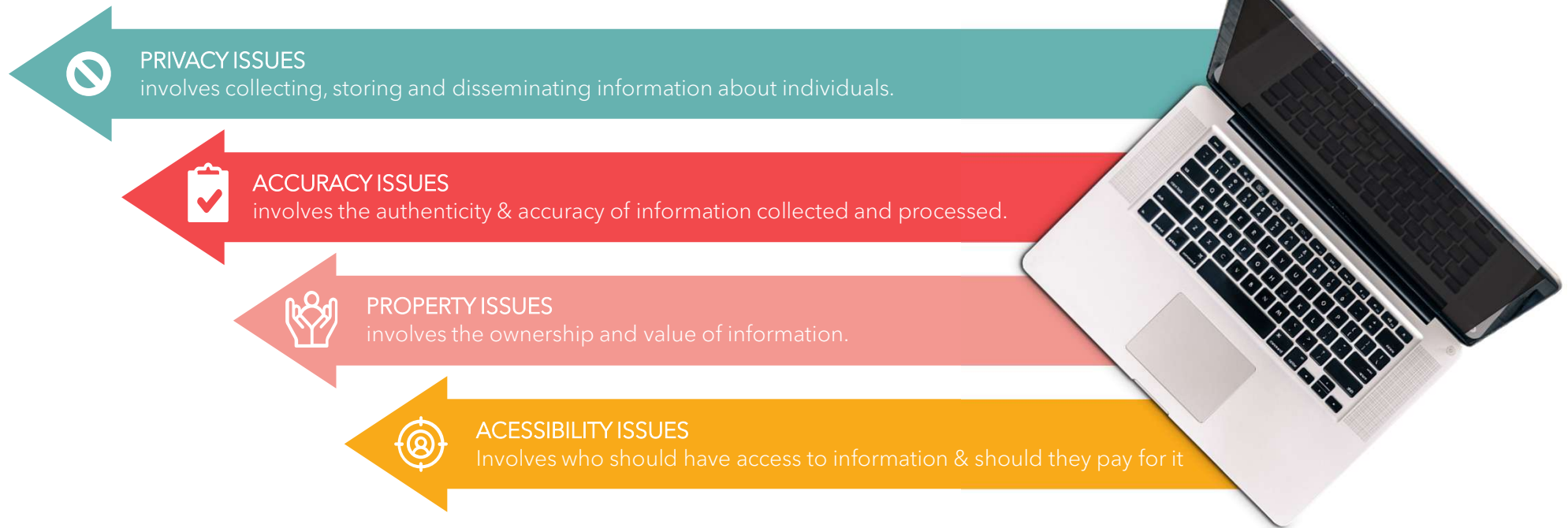
- **Responsibility** : accept the consequences of your decisions and actions
- **Accountability** : determine who is responsible for actions that were taken.
- **Liability** : a legal concept of the right to recover the damages done to them by other individuals or organizations.

Ethical decisions & behaviours can have serious consequences for individuals, organizations, and society.

Unethical is not necessarily *illegal*. In many cases, an individual or organization faced with an ethical decision is not considering whether to break the law.



ETHICAL ISSUES IN INFORMATION TECHNOLOGY



All employees have a responsibility to encourage ethical uses of information and information technology. Organizations require successful ethics programs. Ethical considerations must be incorporated into decision making and managers' behaviours and expectations can strongly influence employees' ethical behaviour

ETHICAL ISSUES FOR IT USERS



IT User refer to person who uses information system components (Data, hardware, software etc.) to deliver organizational benefits or improve productivity.

Some common ethical issues for IT users;

- Software piracy (illegally making copies of software)
- Inappropriate use of computing resources
- Inappropriate sharing of private or confidential information

Thus, organization should develop IT usage policy to set forth the general rights & responsibilities of IT users.

Some best practices of IT usage policy;

- Establishing guidelines for use of company software
- Defining & limiting the appropriate use of IT resources
- Structuring IS to protect data & information
- Installing & maintaining corporate firewall

PRIVACY OF INFORMATION

Information privacy is the right to determine when, and to what extent, information about a person can be gathered or communicated to others.

However, 2 rules also are followed

1. The right of privacy is not absolute. It must be balanced against the needs of society.
2. The public's right to know is superior to the individual's right of privacy.

“

Privacy is the right to be left alone and to be free of unreasonable personal intrusions

”





PROFILING DIGITAL DOSSIERS

On an average day, data about a person is generated in many ways:

Data aggregators or profilers collect public & non-public information data which can be integrated to produce a **digital dossier**, which is an electronic profile of individuals & their habits then sell to whoever need them.

The process of forming a digital dossier is called **profiling**.

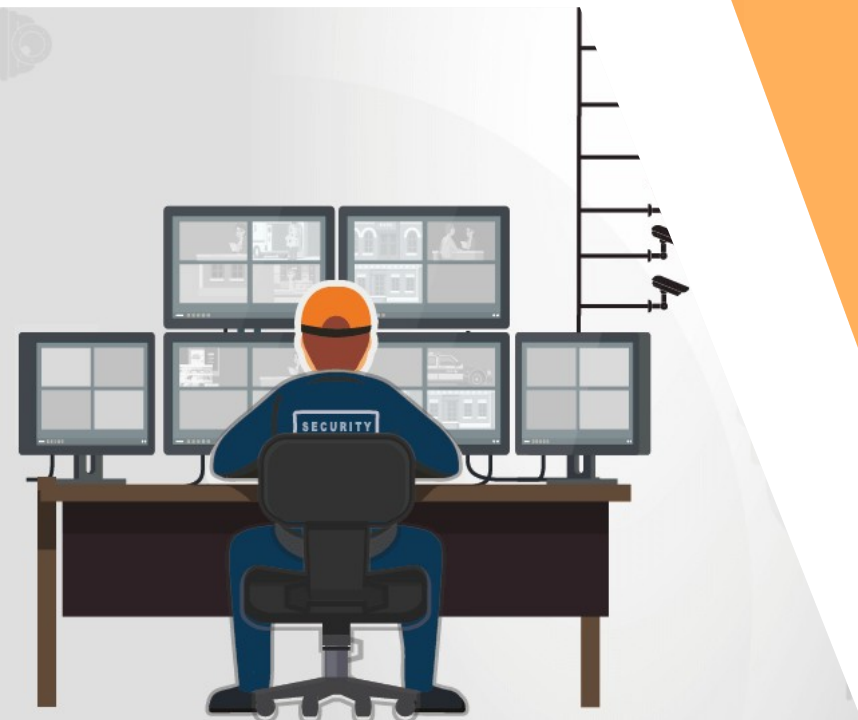
For example, Google is facing lawsuit for allegedly conducting deceptive and misleading tracking practices.

In response, Google contends that all users who sign into Google's services consent to Google's sharing their data with third parties. This process is called **informed consent**.

ELECTRONIC SURVEILLANCE

Tracking people's activities has become a major privacy-related problem

Electronic surveillance is the tracking of people's activities, online or offline, with the aid of information technology. Electronic surveillance is mostly conducted by employers, the government, and other institutions. **Internet-of-thing** technologies such as digital cameras, motion sensors, and biometric readers are facilitated the monitoring of human activity.



GPS sensors & facial recognition in smartphones are routinely geotag photos and videos. Thus, it could be unintentionally supplying criminals with useful intelligence by posting personal images on social networks or photo sharing websites.



PERSONAL INFORMATION IN DATABASE

Personal information is being kept in many databases locations: credit-reporting agencies, banks, utilities company, employers, government agencies, etc.

There are several privacy concerns about the personal information provided to these record keepers;

- Where are the records stored?
- Are the records accurate?
- Under what circumstances will the personal data be released?
- How are the data used?
- To whom are the data given or sold?
- How secure are the data against access by unauthorized people?

PROTECTING PRIVACY

PRIVACY POLICY

An organization's guidelines for protecting the privacy of its customers, business partners, and employees.

OPT-OUT

Informed consent permits the company to collect personal information until the customer specifically requests that the data not be collected.

OPT-IN

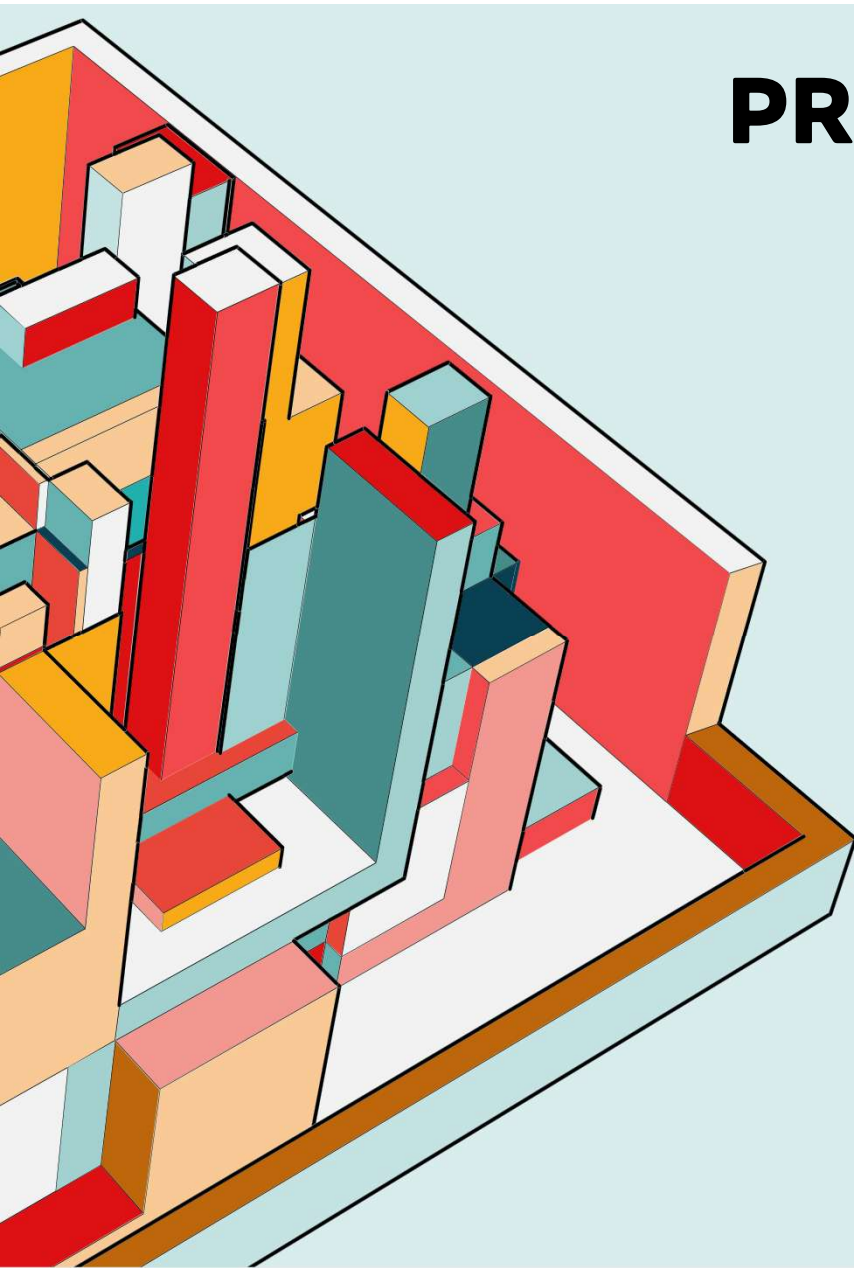
Informed consent prohibits the company to collect any personal information unless the customer specifically authorizes it.

General Data Protection Regulation (GDPR)

Data controllers and data processors should keep minimal data on each data owner, secure it properly, ensure that it is accurate, and retain the data for only as long as it is needed.

Good privacy intentions and managing international data transfer require effective security measures enforces by supply chain governances





PRIVACY POLICY GUIDELINES

Data Collection

- Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.
- Data should be adequate, relevant, and not excessive in relation to the business objective.
- Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).

Data Accuracy

- Sensitive data gathered on individuals should be verified before they are entered into the database.
- Data should be kept current, where and when necessary.
- The file should be made available so that the individual can ensure that the data are correct.
- In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

Data Confidentiality

- Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.
- Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.
- Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.
- Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

INFORMATION SECURITY

Security

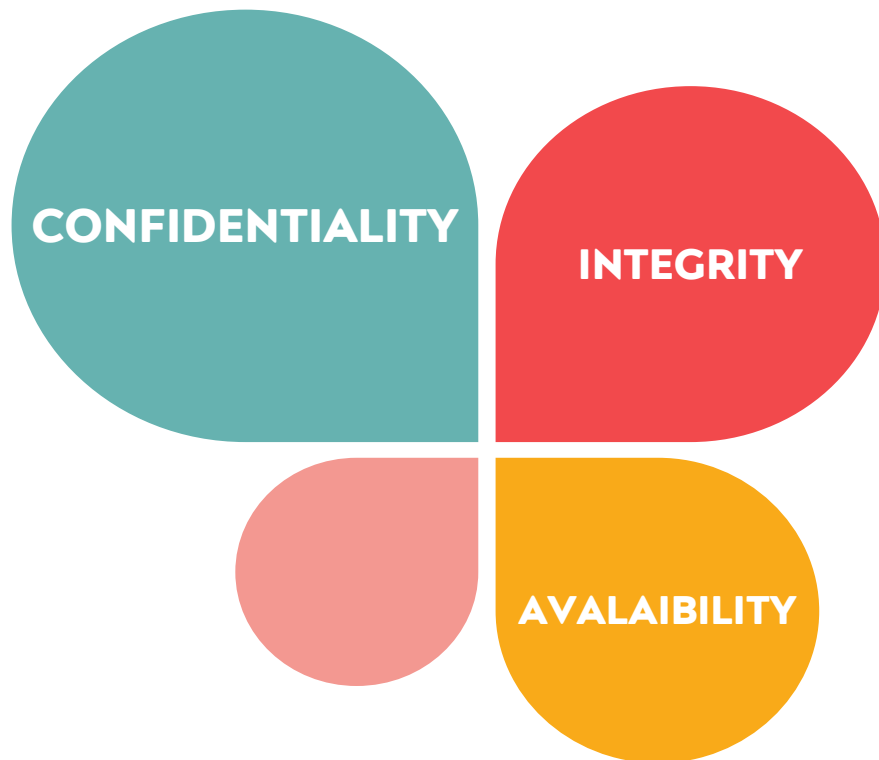


Security

The degree of protection against criminal or harmful activities

Information Security is defined as the protection of information resources from unauthorized access, use, disclosure, disruption, modification, or destruction to provide **Confidentiality**, **Integrity** and **Availability**.

COMPONENTS OF INFORMATION SECURITY



Confidentiality



Keeping data and resources hidden, only those with sufficient privileges may access certain information.

Integrity

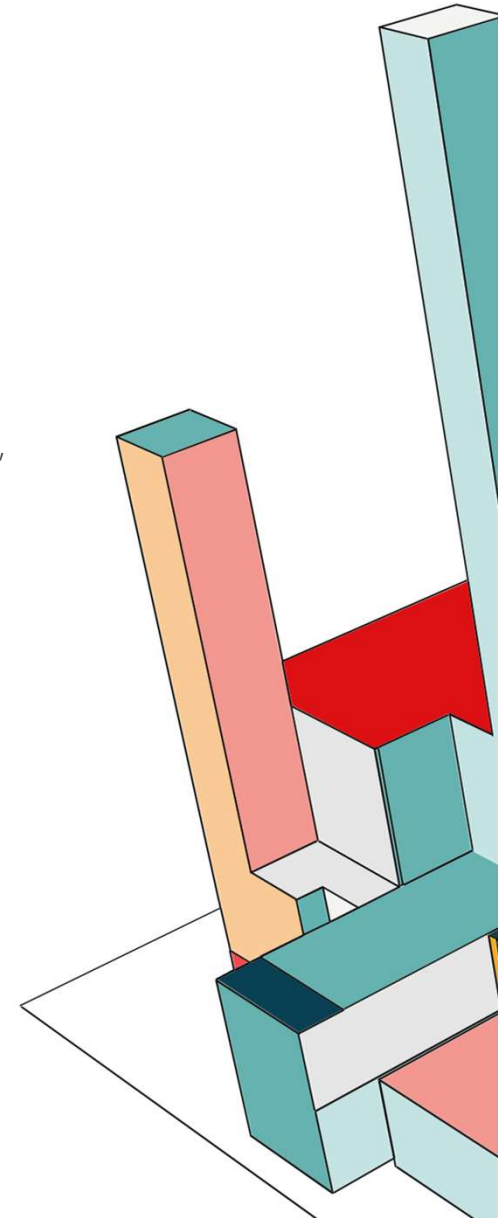


The quality of maintaining accuracy, completeness, & uncorrupted data over the entire storage life cycle.

Availability



Making information accessible to user access without interference or obstruction in the required format.



INFORMATION RESOURCES

Information resources

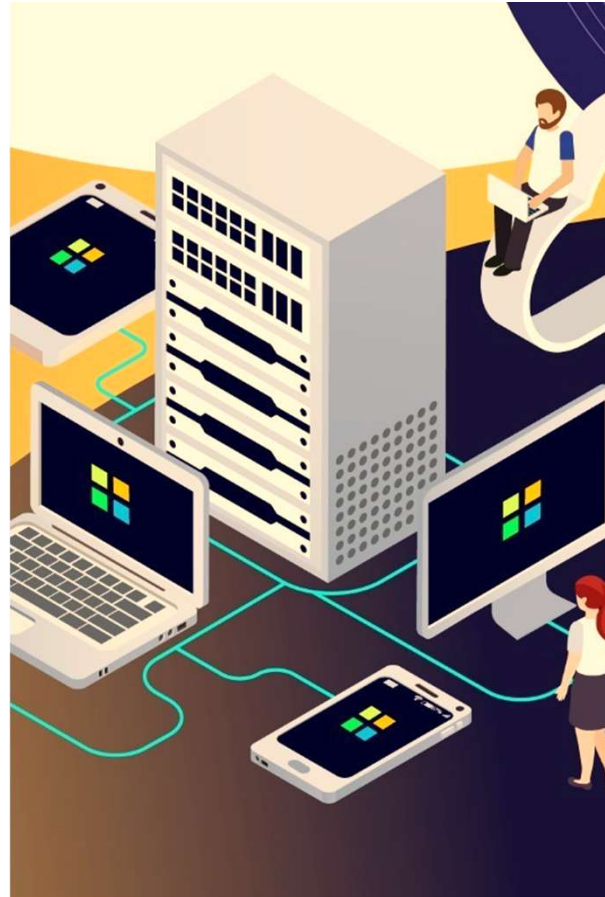
is defined as the available data, system, technology, people, and processes available to perform business. Information resources can be either assets or capabilities.

IT Assets

Tangible or intangible assets that can be used by the company for producing or offering its products

IT Capabilities

Something that is learned or developed over time in order for the company to develop, produce or offer it products.



IT Assets

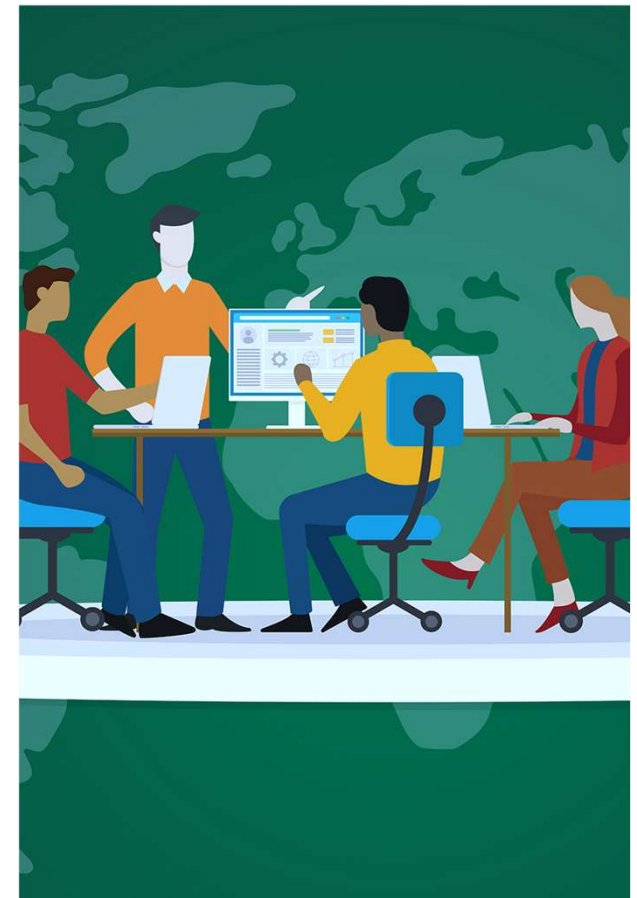
Example:

- IT infrastructure includes data, systems, technology, people, and processes
- Database or Information repository
- Other resources used but not owned

IT Capabilities

Example :

- Technical skills.
- IT management skills
- Relationship skills





SECURITY THREATS

OF INFORMATION , SYSTEM & TECHNOLOGY

Internet is unsecured
It is difficult to perfectly secure
everyone's private information

Despite enormous benefits of information systems & technologies, they also subject to many threats. A **threat** is any danger to which a system may be exposed. The **exposure** is the harm, loss or damage that can result from a threat. A system's **vulnerability** is the possibility that the system will suffer harm by a threat.

THREAT

EXPOSURE

VOLNERABILITY

FACTORS AFFECTING VULNERABILITY

Today, five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them, especially in complex international supply chains:

Interconnected Environment

Today's highly complex interconnected supply chain environment with automation, decentralize & wireless network.



Advanced devices

Smaller, faster and more portable, with greater storage capacity of computer hardware & devices.



Less skills required to be hacker

Internet contains programs called scripts that users with limited skills can download and use for cyber-attacks.



Powerful cybercrime network

Well- organized criminal organizations have taken control of a global billion-dollar crime network.



Lack of management support

Senior managers, who are a critical part of set the tone for security policies, are not taking it seriously enough.



THE THREAT ACTORS

ACTIVIST

Those who have a political message.
Attack to support their cause or
disrupt targeted organizations.

CRIMINALS

Both organized & opportunistic
criminals are those who usually after
material gain & can deploy supporting
tactics for their despicable aims.

SCRIPT KIDDIES & HOBBYISTS

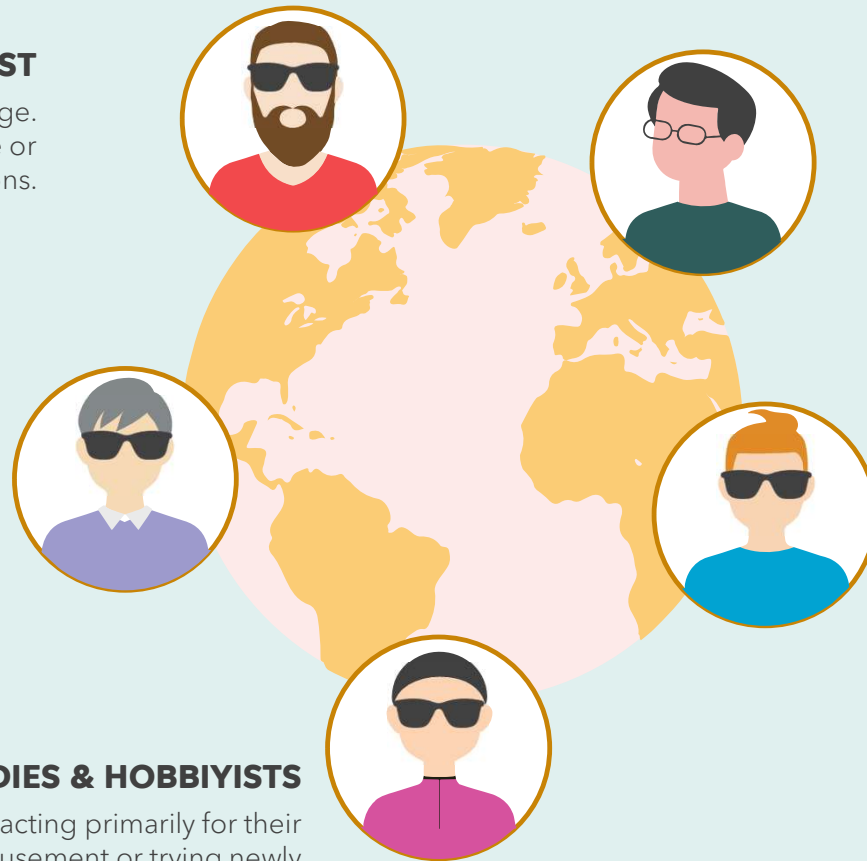
Those who acting primarily for their
own amusement or trying newly
acquired hacking skills

NATION STATES

Develop powerful cyber tools &
techniques to pursue espionage &
disruption of activities in supporting
security, economic or political motives

DISAFFECTED EMPLOYEES

Those who aim to inflict damage,
either on another employee or the
organization. They have good access
& can be very difficult to counter.



ROOT CAUSES OF DATA BREACHES

Human Error

28%

Process Failure

25%

Malicious

47%

Ponemon Institute 2017 Cost of Data Breach Study: Global Analysis

CATEGORIES OF THREATS

HUMAN ERRORS

Unintentional mistakes from laziness, carelessness, or a lack of awareness

SOCIAL ENGINEERING

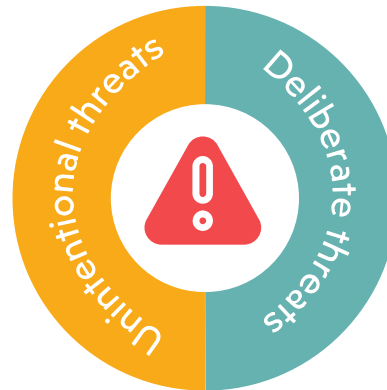
Employees being tricked to providing confidential corporate or personal data

TECHNICAL BREAKDOWN

Systems breakdown from outdated firewalls or overdue security updates

MANAGEMENT FAILURES

Lack of funding for information security efforts



TRESPASS

Unauthorized person illegally attempts to access organizational information

INTELLECTUAL PROPERTY COMPROMISE

Intellectual property e.g. trade secrets, patent & copyright can be pirated & exploit without paying

ALIEN SOFTWARE

Undercover spyware or cookies duplicitously installed on computer to track surfing activities.

SOFTWARE ATTACKS

Malware (Viruses, phishing mails) infect computers through the web to make money

TYPES OF SOFTWARE ATTACKS



Type	Description
Remote Attacks Requiring User Action	
Virus	Segment of computer code that performs malicious actions by attaching to another computer program
Polymorphic virus	Segment of computer code that modifies itself (i.e., changes its computer code) to avoid detection by anti-malware systems, while keeping its same functionality
Worm	Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program)
Phishing attack	Attacks that use deception to acquire sensitive personal information by masquerading as official looking emails or instant messages
Remote Attacks Needing No User Action	
Denial-of-service attack	An attacker sends so many information requests to a target computer system that the target cannot manage them successfully and typically ceases to function (crashes).
Distributed denial-of-service attack	An attacker first takes over many computers, typically by using malicious software. These computers are called <i>zombies</i> or <i>bots</i> . The attacker uses these bots—which form a <i>botnet</i> —to deliver a coordinated stream of information requests to a target computer, causing it to crash.
Attacks by a Programmer Developing a System	
Trojan horse	Software programs that hide in other computer programs and reveal their designed behavior only when they are activated
Back door	Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called a <i>trap door</i>)
Logic bomb	A segment of computer code that is embedded within an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date

PHISHING EXAMPLES

----- Forwarded Message -----

From: PayPal <paypal@notice-access-273.com>

To:

Sent: Wednesday, January 25, 2017 10:13 AM

Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

PayPal

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've placed a limitation on your account.

<http://spapparelsindia.in/Aprons/outlook.com/login.html>

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

Not paypal.com

Log In

[Help](#) | [Contact](#) | [Security](#)

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved

INFORMATION SECURITY IN DIGITAL SUPPLY CHAIN

Figure 21: 2018 Survey Results – Top of Mind Risks of Supply Chain Executives



The 2018 MHI Annual Industry Report Overcoming Barriers to NextGen Supply Chain Innovation

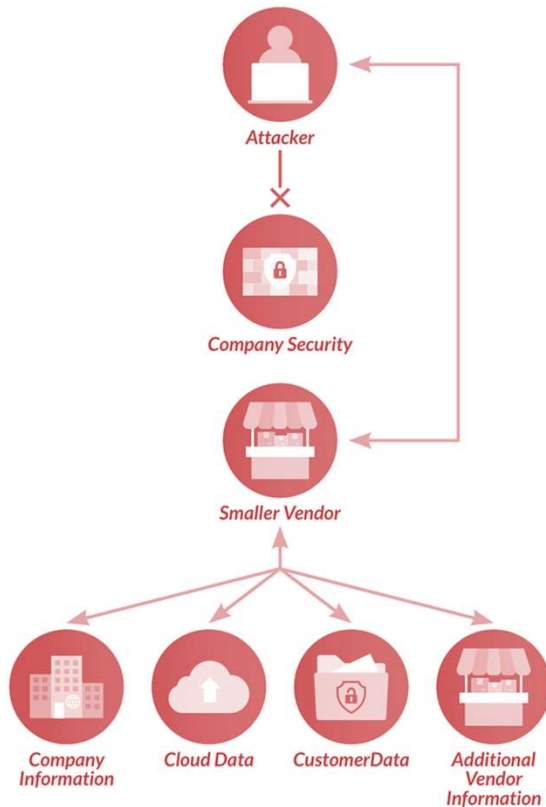
In the era of digital supply chain, core activities e.g. manufacturing & logistics are outsourced to 3rd party providers

This approach bring with it a growing complex cyber-security risks – and no company is immune. There have already been widely publicized cyber-attacks on well-known companies that not only hurt their financial performance but also harmed their customers and significantly sabotage their reputations.

Outsourcing robotic process automation, cloud-base solutions & systems, analytic software-as-a-solution, and internet-of-things solutions adding explosion of supply chain vulnerabilities for cybercrimes.

HOW SUPPLY CHAIN ATTACK WORK

Attackers bypass large organization's cybersecurity & data protections by attacking smaller vendors to access larger company's information, their customers, and other vendors.

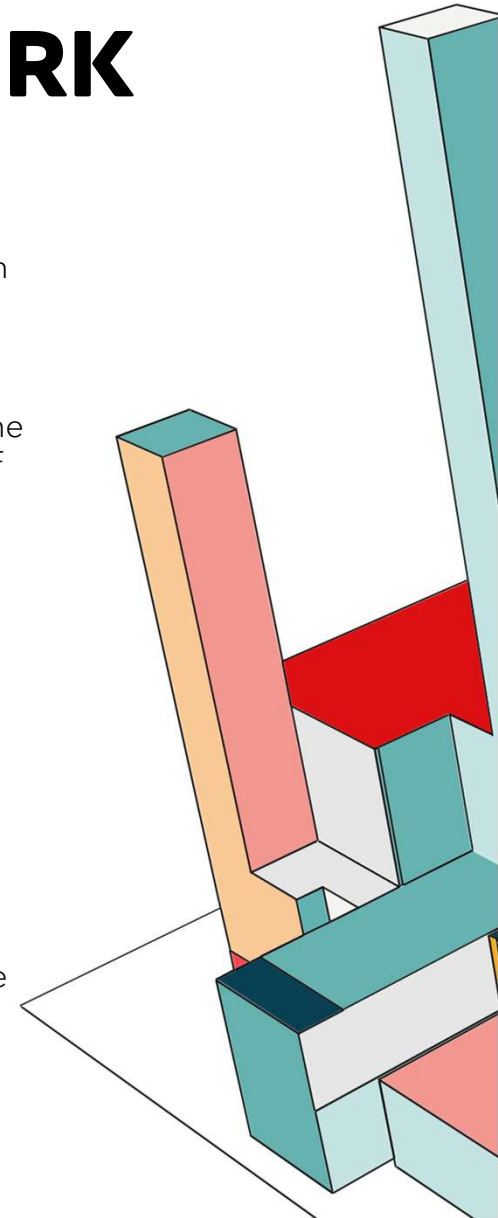


Third-Party Vendor Attacks, also known as Supply Chain Attacks, are typically attacks that fall into one of the primary root causes of a compromise.

What makes them unique is the target is not data owned by the breached organization but rather aimed for the information of the business clients or other vendors in a supply chain.

Rather than attack a single large organization – a large multi-national corporation with a well-resourced cybersecurity program, for example – identity criminals will attack a smaller vendor with less security protections that supports the same large multi-national company along with many other businesses.

A supply chain attack can come in the form of breaching a single organization and stealing information from multiple companies or using flaws in a single product or service used by multiple companies to access the personal information stored in their databases



SUPPLY CHAIN POINTS OF PENETRATION



Assess supply chain vulnerability

To effectively allocate security resources, organisations need to know the vulnerable points of the supply chain network where these cyber risks are most likely to penetrate. More than half of malicious cyber-attacks target smaller organisations due to the lack of adequate protection measures installed in their information systems.

Key failure points



Technical PoP

IT assets are prone to cyber risks including hardware, systems, software, and personnel. E.g. outdated & poorly maintained systems, outsourcing servers



Human PoP

Human resources could expose a threats willingly or unintentionally. This vulnerability is then intensified with human insecurely interactions across supply chain organizations



Physical PoP

Physical objects & infrastructures are vulnerable for cyber risks & other risks e.g. natural disaster that could impact to cyber systems and disrupt supply chain flows

SUPPLY CHAIN CYBER ATTACK

British airway magecart attack

In 2018, attackers compromised a BA network account issued to an employee of cargo-handling firm [Swissport](#) before planting card-skimming malware on the airline's payments page.

Credentials for an administration console were hacked allowed cyber criminals to manipulate partial of BA's website so that data entered into the site was sent to cyber criminals. Moreover, scripts related to the British Airways baggage claim form were hacked so that data was also transferred to hackers. The data stolen included payment card data (including Card Verification Value codes) and travel booking details as well as customer name and address information.

Data of more than 380,000 customers was stolen as the breach went undetected for 16 days.

BA was fined with an enormous of £183m for violations of GDPR data protection regulations



SUPPLY CHAIN CYBER ATTACK

SolarWinds supply chain attack

In 2020, a hacking operation injected malicious code into SolarWinds' software development process, specifically the Orion software updates. The attackers could infiltrate SolarWinds' build systems and insert malware, which spread among customers as part of legitimate software updates.

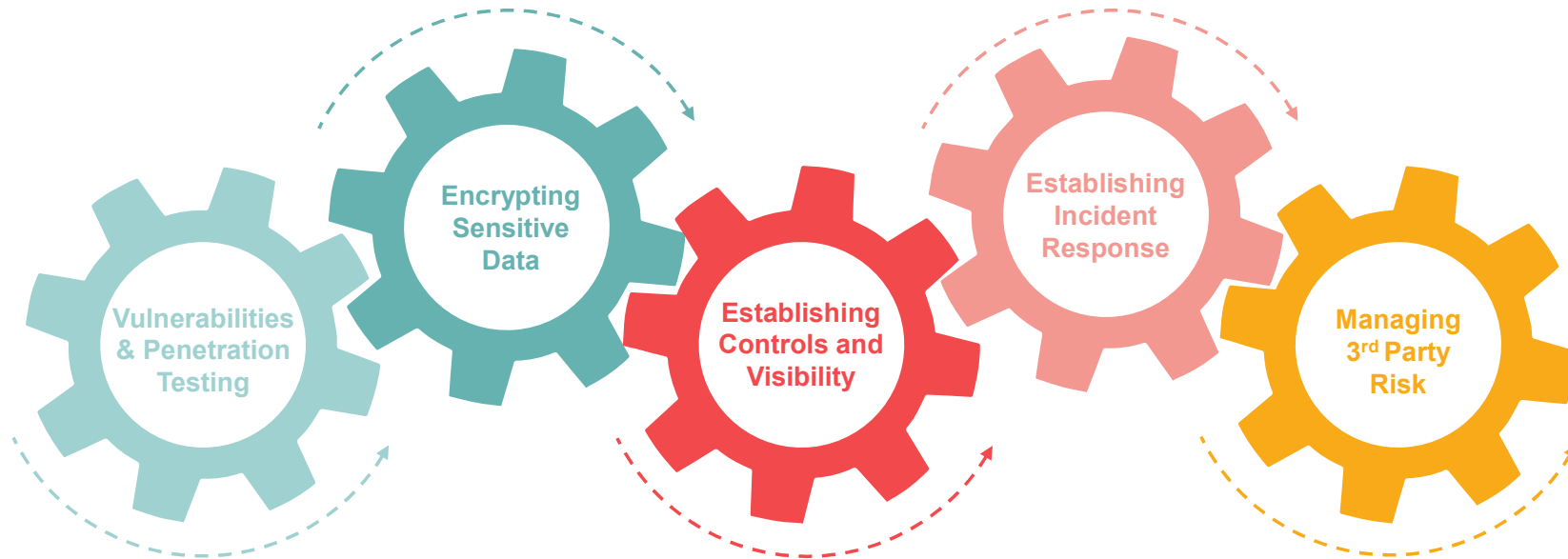
The attack allowed the attackers to access sensitive data and systems of numerous organizations that used Orion platform, including key US government agencies, Microsoft, Intel, Accenture, Cisco and numerous Fortune 500 companies. Due to the malicious code inserted during the build process of the software update and the malicious injection occurred early in the supply chain, even though it was delivered to customers via secure signing and verification checks, it couldn't be detected.

It took almost 15 months to discover the breach.

SolarWinds claimed it spent £18m to "investigate and remediate the cyber incident,"



BEST PRACTICES FOR SUPPLY CHAIN CYBER RISKS MITIGATION



Vulnerabilities & Penetration Testing

Vulnerability scans enable early detection of potential risks. The penetration test results ensure the effectiveness of security protocols.

Encrypting Sensitive Data

Identify supply chain sensitive information & private data, then secure them with encryption technology e.g. digital signatures, multi-authentication

Establishing Controls and Visibility

Leveraging tools to control role- and user-based access to cover all supply chain partners with Identity & access management security practices.

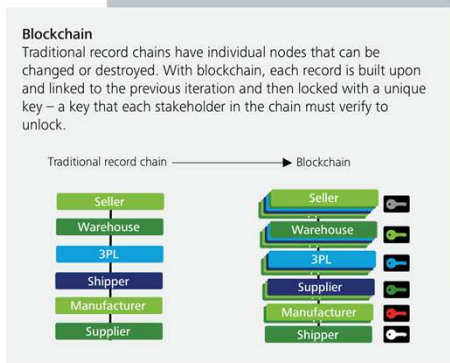
Establishing Incident Response

Proactively prepare for SC disruption with an effective incident response plan to minimize impacts & prevent recurrence of cyber attacks.

Managing 3rd Party Risk

Sharing 3rd party risk assessments with SC stakeholders to collaborate protecting SC valuable IT assets. Executives buy-in is important.

CYBER RISKS MITIGATION: BLOCKCHAIN

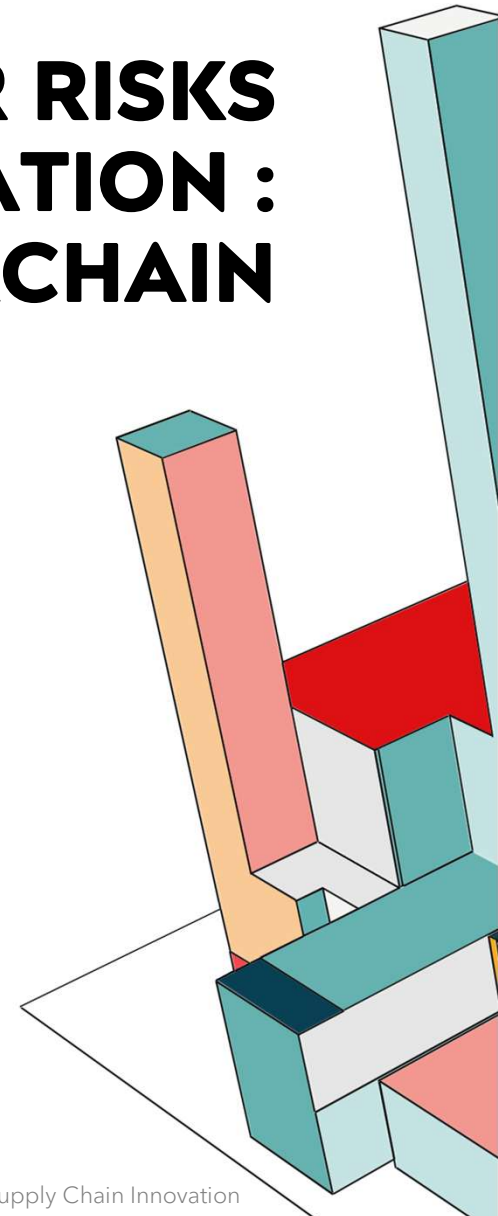


Blockchain has a great potential to secured connection and data sharing in supply chain – without compromising security and privacy.



What Leaders Should Be Doing

- Consider how having access to more data (both upstream and downstream) could change your strategy and operations
- Develop and execute risk profile and vulnerability assessments
- Develop business continuity and contingency plans
- Establish a robust data management plan and records retention program
- Explore the potential applications for blockchain in your supply chain and initiate a pilot project; start with the parts of your organization that require the highest levels of trust
- Work with suppliers to improve visibility to cyber risks and collaborate on security measures (e.g., reviewing certifications of Tier 1 - Tier N suppliers)
- Conduct penetration tests that attempt to hack your systems in a controlled environment
- Explore the potential applications for blockchain in your supply chain (Look at your organization from the perspective of trust. Determine which parts of your operations require the highest levels of trust. Seek new partners based on confidence in their data and their promises. If you work with intermediaries whose only role is to “certify” trust, consider blockchain as a better and cheaper alternative.)



An abstract graphic in the top right corner consisting of various 3D rectangular blocks and bars in shades of orange, teal, and light blue, arranged in a scattered, architectural-like pattern.

INTERNET PROTECTION



Search
Engine
Safety



Web
Content
Filter



Secure
HTTPS//



Public
Wi-Fi



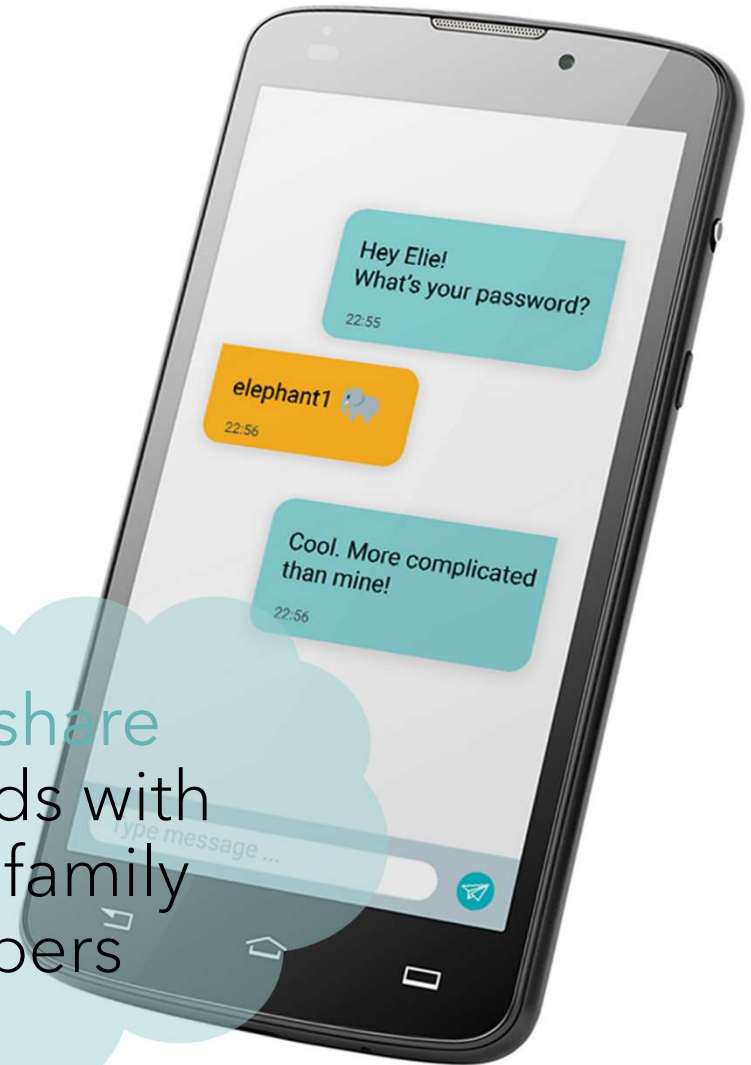
Internet
of Things

PASSWORD EXPOSURE => PROBLEM

Document or
sticky note with
passwords
written on it

my
password
elephant1

Freely share
passwords with
friends, family
members



DATA BREACHES LEAD TO PASSWORD PROBLEMS BECAUSE...

Example

Password that was stolen
was *elephant*

Password required by
website is 8 characters 1
symbol

32 symbols on the
computer(would take a
human 5 minutes)

Computers can carry out
these tasks in fractions
of a second



PASSWORDS SOMETIMES ARE
EXTRACTED



VERY SIMPLE TO TRY ALL
ALTERNATIVE OPTIONS OF
PASSWORD-BASE



SECURITY QUESTIONS

Typically, users are honest when filling out security questions.

Malicious parties can utilize social media to find out the answers to these questions, which allows them to reset your password.

Best practice is to not be honest when filling out these questions. Treat security questions as another password field.

TWO-FACTOR AUTHENTICATION (2FA)

As opposed to the standard password authentication, 2FA OTP (one-time password) uses two elements. These are "*something that user knows*," such as a password or a PIN code, and "*something that user has*," typically a mobile phone or hardware token.

Used in combination, they provide greatly enhanced security for data access.

2FA solves the problem of:

- Data breach through weak or stolen passwords
- User-created passwords that are not random
- Re-use of passwords intended for access to company assets for private accounts
- Passwords containing user-specific data - e.g. name, date of birth
- Simple patterns to derive new passwords, such as "elephant1," "elephant2," etc.



Your Role and Responsibility in Protecting Data

**Be
Strategic
With
Credentials**



Do

- Create passwords that are long and strong, using at least 8-12 characters, upper- and lowercase letters, numbers, and symbols.
- Change your password often. (General rule of thumb: Change passwords every 90 days.)



Don't

- Use information that can be easily found about you online or otherwise.
- Share passwords with others.
- Store your passwords online.
- Use any part of your Social Security Number, birth date, or other personal data when creating passwords.

Your Role and Responsibility in Protecting Data

Surf
Internet
Safely



Do

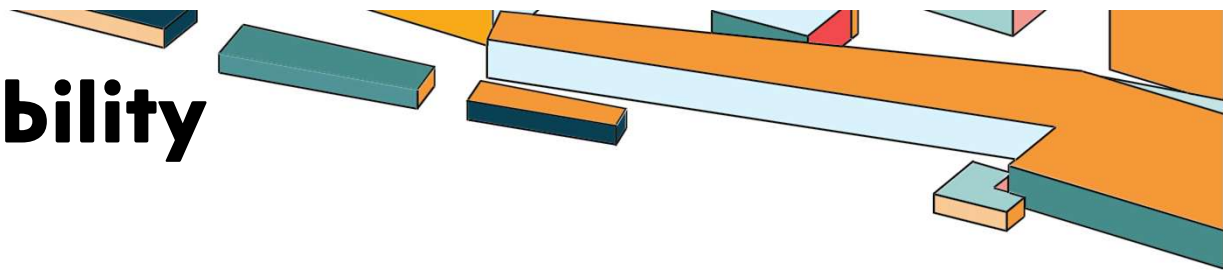
- Use wireless networks you trust and know are protected.
- Be cautious when using public computers.
- Ensure you are downloading legitimate apps from trusted publishers.
- Be aware that secure websites start with **https**, not http.
- Be sure to log out completely (which terminates access) when exiting all websites to prevent cybercriminals from obtaining your personal information.
- Hover over questionable links to reveal the true destination before clicking.



Don't

- Use public computers to access confidential information or accounts, or to perform financial transactions.
- Click on websites you don't know or on pop-up ads or banners.
- Click on links or attachments from unknown sources.

Your Role and Responsibility in Protecting Data



Protect IT & Intellectual Assets



Do

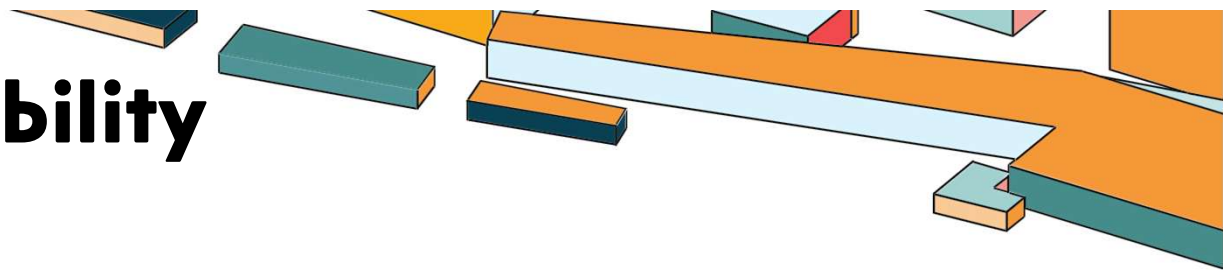
- Be aware of suspicious phone calls, emails and texts requesting access/changes to personal identifiable information, funds disbursement requests, etc. Be sure to validate that the source number or email matches what we have on file for the client.
- Follow company verification and authentication protocols – no exceptions.
- Educate our business partners:
 - on security authentication policies and procedures so they know what to expect
 - to review credit card, cell phone and financial statements on a regular basis.
 - to contact their financial institutions or services providers as soon as they suspect something suspicious.



Don't

- Take shortcuts or veer from firm policies and procedures.
- Respond to requests for personal information from an unsolicited email or from an unsolicited incoming phone call.
- Do not act on email-based requests for sensitive information, money movements, or trading.

Your Role and Responsibility in Protecting Data



Limit What To Share Online



Do

- Ensure that any firm and/or client information that you are entering online is with an individual or vendor/third-party authorized by the firm.
- Educate our business partners:
 - to be very selective about the information they choose to share on social media and with whom they choose to share it.
 - to keep their personal information private (home address, phone number, and birthdate).
 - to set privacy and security settings on web services and devices to your comfort level for sharing.



Don't

- Do not share any firm or client information on any unauthorized site.
- Do not talk about our clients on social media.
- Do not post personal information about family, friends, clients, co-workers online.
- Do not share information that could help a fraudster gain access to accounts or impersonate the client.

A close-up photograph of a person's hands holding a black smartphone. The person is wearing a grey t-shirt. A teal rectangular box is overlaid on the left side of the image, containing white text. The background is blurred, showing what appears to be a retail or office environment.

Security is everyone's
RESPONSIBILITY

THANK YOU