UNIT-V

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

- Introduction
- Cost of Cyber Crimes
- IPR Issues
- Web Threats for Organizations
- Security and Privacy Implications
- Social Media Marketing: Security Risks
- Perils for Organizations
- Social Computing and associated challenges for organizations.

Organizational Implications-Introduction

In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices or intense scans from criminal groups.

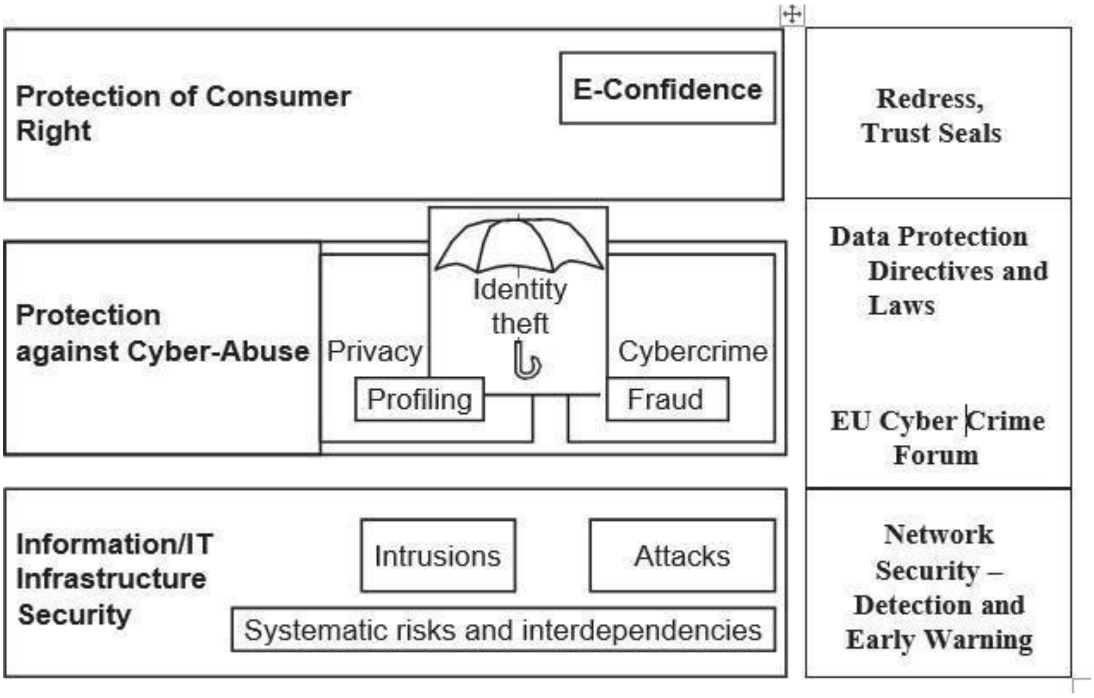

Protection of Consumer Right
E-Confidence
Redress, Trust Seals
Protection against Cyber-Abuse
Privacy
Identity theft
Cybercrime
Profiling
Fraud
Data Protection Directives and Laws
EU Cyber Crime Forum
Information/IT Infrastructure Security
Intrusions
Attacks
Systematic risks and interdependencies
Network Security – Detection and Early Warning

Fig: A cyber security perspective. EU is the European Union.

PI is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual.

Most information the organization collects about an individual is likely to come under "PI" category if it can be attributed to an individual. For an example, PI is an individual's first name or first initial and last name in combination with any of the following data:

1. Social security number (SSN)/social insurance number.
2. Driver’s license number or identification card number.
3. Bank account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual’s financial account.
4. Home address or E-Mail address.
5. Medical or health information.

An insider threat is defined as “the misuse or destruction of sensitive or confidential information, as well as IT equipment that houses this data by employees, contractors and other ‘trusted’ individuals.”

Insider threats are caused by human actions such as mistakes, negligence, reckless behavior, theft, fraud and even sabotage. There are three types of “insiders” such as:

1. A malicious insider is motivated to adversely impact an organization through a range of actions that compromise information confidentiality, integrity and/or availability.
2. A careless insider can bring about a data compromise not by any bad intention but simply by being careless due to an accident, mistake or plain negligence.
3. A tricked insider is a person who is “tricked” into or led to providing sensitive or private company data by people who are not truthful about their identity or purpose via “pretexting” (known as social engineering).

- **Insider Attack Example 1: Heartland Payment System Fraud**

  A case in point is the infamous “Heartland Payment System Fraud” that was uncovered in January 2010. This incident brings out the glaring point about seriousness of “insider attacks. In this case, the concerned organization suffered a serious blow through nearly 100 million credit cards compromised from at least 650 financial services companies. When a card is used to make a purchase, the card information is trans- mitted through a payment network.

- **Insider Attack Example 2: Blue Shield Blue Cross (BCBS)**

  Yet another incidence is the Blue Cross Blue Shield (BCBS) Data Breach in October 2009 the theft of 57 hard drives from a BlueCross BlueShield of Tennessee training facility puts the private information of approximately 500,000 customers at risk in at least 32 states. The two lessons to be learnt from this are:

  1. Physical security is very important.
  2. Insider threats cannot be ignored.

What makes matters worse is that the groups/agencies/entities connected with cybercrimes are all linked. There is certainly a paradigm shift in computing and work practices; with workforce mobility, virtual teams, social computing media, cloud computing services being offered, sharp rise is noticed in business process outsourcing (BPO) services, etc. to name a few.

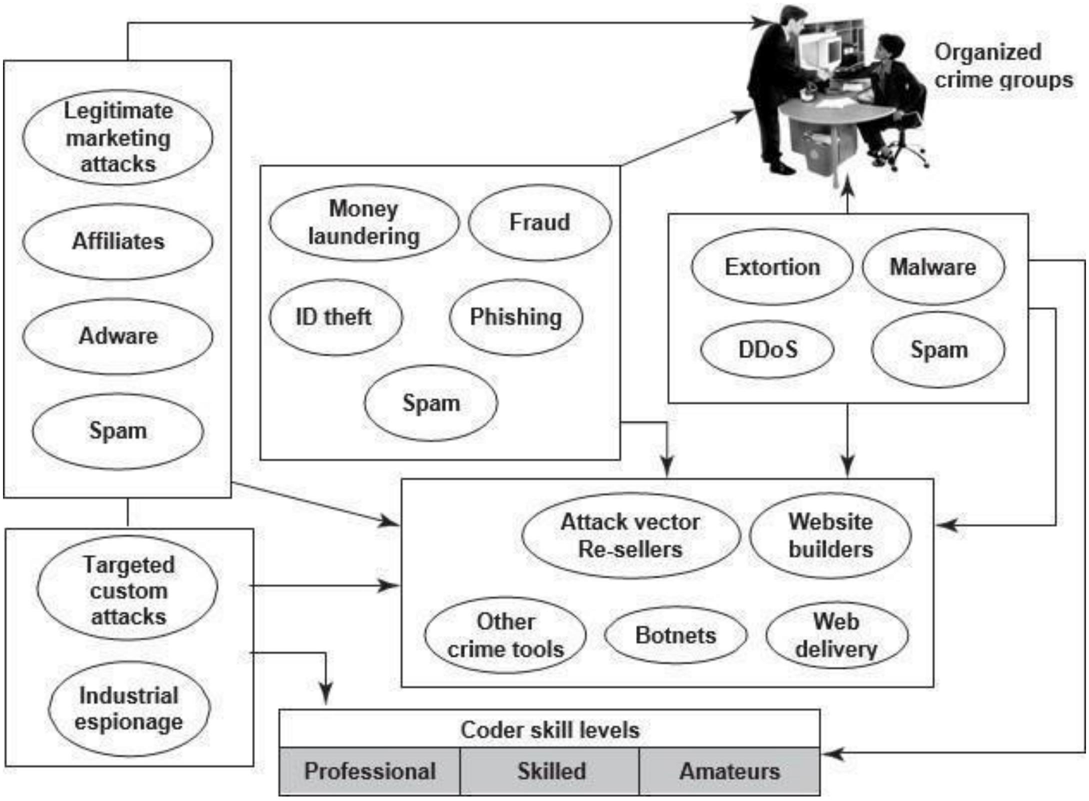


Fig: Cybercrimes – the flow and connections.

A key message from this discussion is that cybercrimes do not happen on their own or in isolation. Cybercrimes take place due to weakness of cybersecurity practices and “privacy” which may get impacted when cybercrimes happen.

Privacy has following four key dimensions:

1. **Informational/data privacy:** It is about data protection, and the users’ rights to determine how, when and to what extent information about them is communicated to other parties.
2. **Personal privacy:** It is about content filtering and other mechanisms to ensure that the end-users are not exposed to whatever violates their moral senses.
3. **Communication privacy:** This is as in networks, where encryption of data being transmitted is important.
4. **Territorial privacy:** It is about protecting users’ property for example, the user devices from being invaded by undesired content such as SMS or E-Mail/Spam messages. The paradigm shift in computing brings many challenges for organizations; some such key challenges are described here.

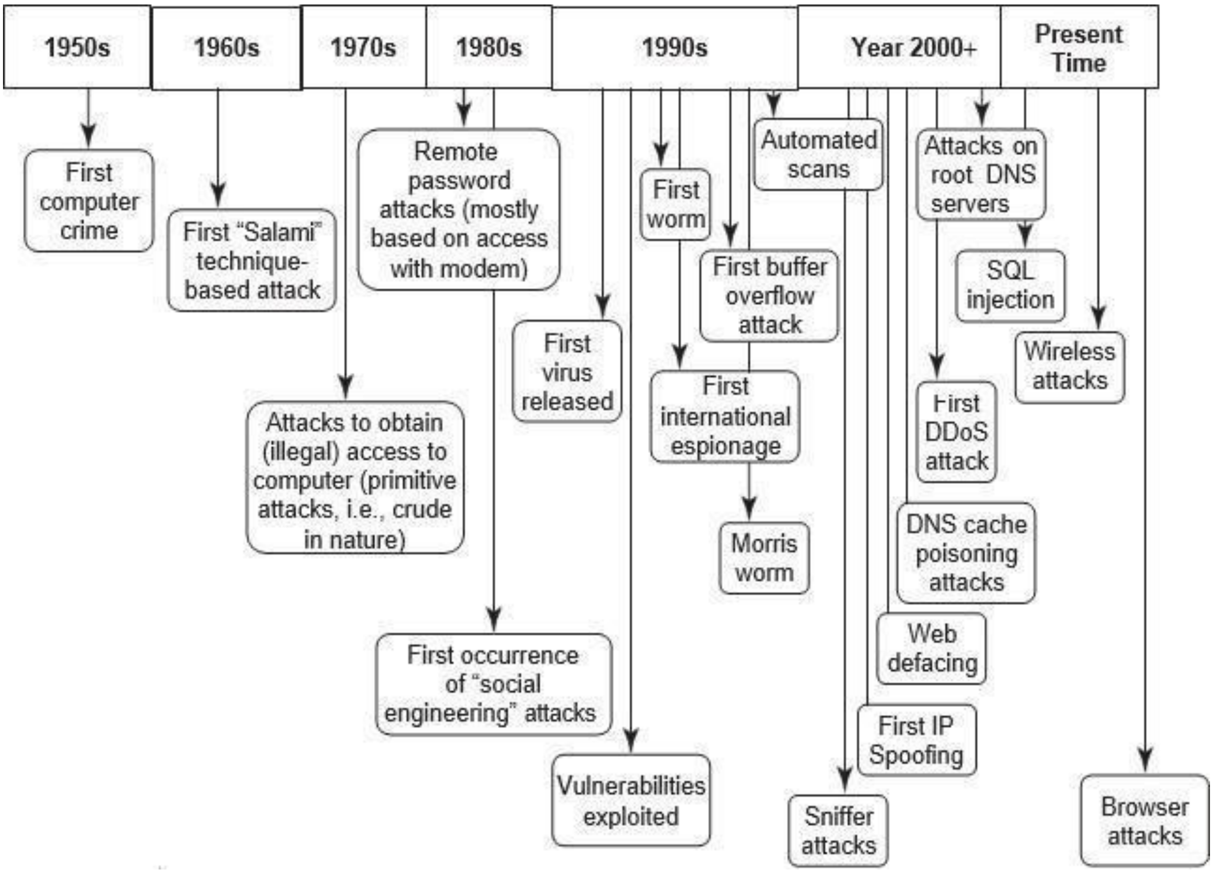

1950s
1960s
1970s
1980s
1990s
Year 2000+
Present Time
First computer crime
First "Salami" technique-based attack
Remote password attacks (mostly based on access with modem)
Attacks to obtain (illegal) access to computer (primitive attacks, i.e., crude in nature)
First occurrence of "social engineering" attacks
First virus released
Vulnerabilities exploited
First worm
First international espionage
First buffer overflow attack
Morris worm
Automated scans
Sniffer attacks
First IP Spoofing
Web defacing
DNS cache poisoning attacks
Attacks on root DNS servers
First DDoS attack
SQL injection
Wireless attacks
Browser attacks

Fig: Security threats – paradigm shift.

The key challenges from emerging new information threats to organizations are as follows:

1. **Industrial espionage:** There are several tools available for web administrators to monitor and track the various pages and objects that are accessed on their website.
2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based "cloaking":** Businesses are global in nature and economies are interconnected.
4. **Cyberterrorism:** "Cyberterrorism" refers to the direct intervention of a threat source toward your organization's website.

Confidential information leakage: "Insider attacks" are the worst ones. Typically, an organization is protected from external threats by your firewall and antivirus solutions cybercrimes cost a lot to organizations.

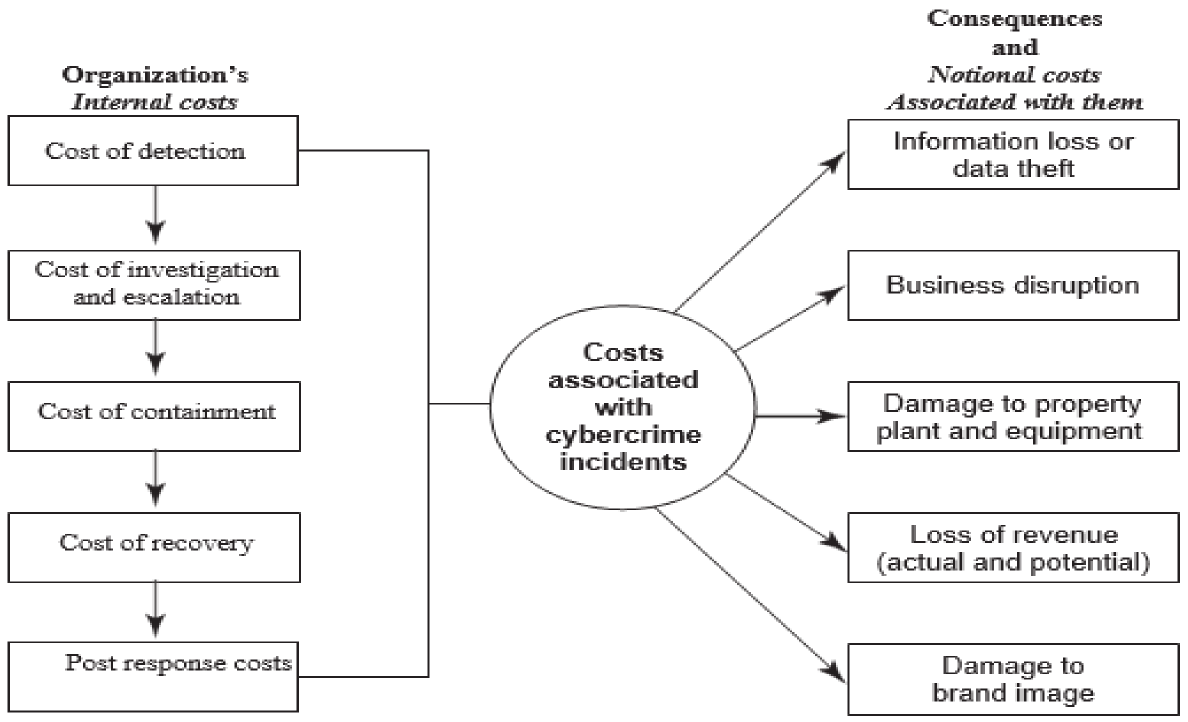

Organization's
Internal costs
Cost of detection
Cost of investigation and escalation
Cost of containment
Cost of recovery
Post response costs
Costs associated with cybercrime incidents
Consequences and Notional costs Associated with them
Information loss or data theft
Business disruption
Damage to property plant and equipment
Loss of revenue (actual and potential)
Damage to brand image

Fig: Cost of cybercrimes.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

Detection and recovery constitute a very large percentage of internal costs. This is supported by a benchmark study conducted by Ponemon Institute USA carried out with the sample of 45 organizations representing more than 10 sectors and each with a head count of at least 500 employees.

- **Organizations have Internal Costs Associated with Cyber security Incidents**

The internal costs typically involve people costs, overhead costs and productivity losses. The internal costs, in order from largest to the lowest and that has been supported by the benchmark study mentioned:

1. Detection costs.(25%)
2. Recovery costs.(21%)
3. Post response costs.(19%)

4. Investigation costs.(14%)
5. Costs of escalation and incident management.(12%)
6. Cost of containment.(9%)

- **The consequences of cybercrimes and their associated costs, mentioned**
  1. Information loss/data theft.(42%)
  2. Business disruption.(22%)
  3. Damages to equipment, plant and property.(13%)
  4. Loss of revenue and brand tarnishing.(13%)
  5. Other costs.(10%)
- **The impact on organizations by various cyber crimes**
  1. Virus,worms and Trojans-100%
  2. Malwares-80%
  3. Botnets-73%
  4. Web based attacks-53%
  5. Phishing and Social engineering-47%
  6. Stolen devices-36%
  7. Malicious insiders-29%
  8. Malicious code-27%
- **Average days taken to resolve cyber Attacks**
  1. Attacks by Malicious insiders-42 days
  2. Malicious code-39 days
  3. Web based attacks-19 days
  4. Data lost due to stolen devices-10 days
  5. Phishing and social engineering attacks-9 days
  6. Virus,worms,and trojans-2.5 days
  7. Malware-2 days
  8. Botnets- 2 days

Among the other reasons for the growth in the cost of cybercrime:

- Cybercriminals are embracing new attack technologies.
- Many new Internet users come from countries with weak cybersecurity.
- Online crime is becoming easier through cybercrime-as-a-service and other business schemes.
- Cybercriminals are becoming more financially sophisticated, making it easier to monetize their exploits.
  - **There are many new endpoints in today's complex networks; they include hand-held devices.**

    Again, there are lessons to learn:

    1. **Endpoint protection:** It is an often-ignored area but it is IP-based printers, although they are passive devices, are also one of the endpoints.

2. **Secure coding:** These practices are important because they are a good mitigation control to protect organizations from “Malicious Code” inside business applications.
3. **HR checks:** These are important prior to employment as well as after employment.
4. **Access controls:** These are always important, for example, shared IDs and shared laptops are dangerous.
5. **Importance of security governance:** It cannot be ignored policies, procedures and their effective implementation cannot be over-emphasized.

- **Organizational Implications of Software Piracy**

Use of pirated software is a major risk area for organizations.

From a legal standpoint, software piracy is an IPR violation crime. Use of pirated software increases serious threats and risks of cybercrime and computer security when it comes to legal liability.

The most often quoted reasons by employees, for use of pirated software, are as follows:

1. Pirated software is cheaper and more readily available.
2. Many others use pirated software anyways.
3. Latest versions are available faster when pirated software is used.

Web Threats for Organizations: The Evils and Perils

Internet and the Web is the way of working today in the interconnected digital economy. More and more business applications are web based, especially with the growing adoption of cloud computing.

- **Overview of Web Threats to Organizations**

The Internet has engulfed us! Large number of companies as well as individuals have a connection to the Internet. Employees expect to have Internet access at work just like they do at home.

IT managers must also find a balance between allowing reasonable personal Internet use at work and maintaining office work productivity and work concentration in the office.

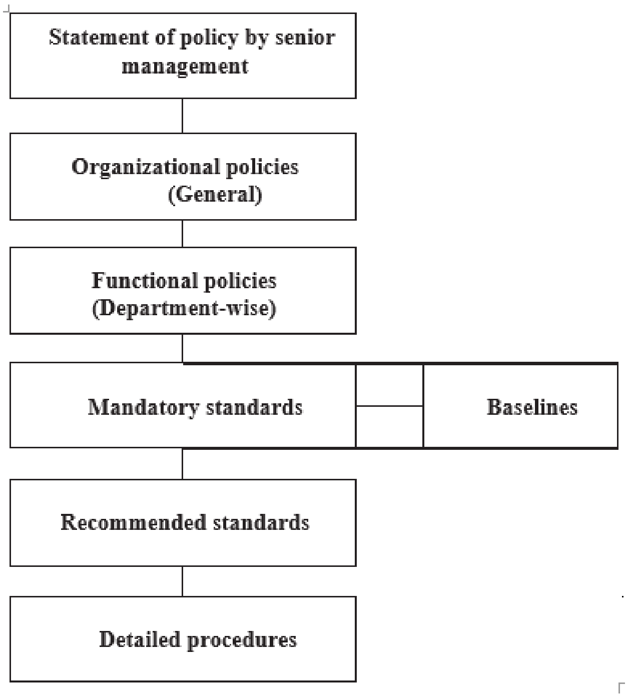
- **Employee Time Wasted on Internet Surfing**

This is a very sensitive topic indeed, especially in organizations that claim to have a “liberal culture.” Some managers believe that it is crucial in today’s business world to have the finger on the pulse of your employees.

People seem to spend approximately 45-60 minutes each working day on personal web surfing at work.

- **Enforcing Policy Usage in the Organization**

  An organization has various types of policies. A security policy is a statement produced by the senior management of an organization, or by a selected policy board or committee to dictate what type of role security plays within the organization.



Statement of policy by senior management
Organizational policies (General)
Functional policies (Department-wise)
Mandatory standards
Baselines
Recommended standards
Detailed procedures

Fig: Policy hierarchy chart.

- **Monitoring and Controlling Employees' Internet Surfing**

  A powerful deterrent can be created through effective monitoring and reporting of employees' Internet surfing.

  Even organizations with restrictive policies can justify a degree of relaxation; for example, allowing employees to access personal sites only during the lunch hour or during specified hours.

- **Keeping Security Patches and Virus Signatures Up to Date**

  Updating security patches and virus signatures have now become a reality of life, a necessary activity for safety in the cyberworld! Keeping security systems up to date with security signatures, software patches, etc. is almost a nightmare for management.

- **Surviving in the Era of Legal Risks**

  As website galore, most organizations get worried about employees visiting inappropriate or offensive websites. We mentioned about Children's Online Privacy Protection.

  Serious legal liabilities arise for businesses from employee's misuse/inappropriate use of the Internet.

- **Bandwidth Wastage Issues**

  Today's applications are bandwidth hungry; there is an increasing image content in messages and that too, involving transmission of high-resolution images.

There are tools to protect organization's bandwidth by stopping unwanted traffic before it even reaches your Internet connection.

- **Mobile Workers Pose Security Challenges**

  Use of mobile handset devices in cybercrimes. Most mobile communication devices for example, the personal digital assistants has raised security concerns with their use. Mobile workers use those devices to connect with their company networks when they move. So the organizations cannot protect the remote user system as a result workforce remains unprotected. We need tools to extend web protection and filtering to remote users, including policy enforcement

- **Challenges in Controlling Access to Web Applications**

  Today, a large number of organizations' applications are web based. There will be more in the future as the Internet offers a wide range of online applications, from webmail or through social networking to sophisticated business applications. Employees use personal mail id to send business sensitive information (BSI) for valid or other reasons. It leads to data security breach. The organizations need to decide what type of access to provide to employees.

- **The Bane of Malware**

  Many websites contain malware. Such websites are a growing security threat. Although most organizations are doing a good job of blocking sites declared dangerous, cyber attackers, too, are learning. Criminals change their techniques rapidly to avoid detection.

- **The Need for Protecting Multiple Offices and Locations**

  Delivery from multi-locations and teams collaborating from multi-locations to deliver a single project are a common working scenario today. Most large organizations have several offices at multiple locations. In such scenario Internet-based host service is best idea to protect many locations.

Security and privacy implications from cloud computing

Cloud computing is one of the top 10 Cyber Threats to organizations. There are data privacy risks through cloud computing. Organizations should think about privacy scenarios in terms of "user spheres". There are three kinds of spheres and their characteristics:

1. **User sphere:** Here data is stored on users' desktops, PCs, laptops, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to users and monitor that access to ensure misuse does not happen.
2. **Recipient sphere:** Here, data lies with recipients: servers and databases of network providers, service providers or other parties with whom data recipient shares data. Organizations

responsibility is to minimize users privacy risk by ensuring unwanted exposure of personal data of users does not happen

3. **Joint sphere:** Here data lies with web service provider's servers and databases. This is the in between sphere where it is not clear to whom does the data belong. Organization responsibility is to provide users some control over access to themselves and to minimize users futures privacy risk.

7 Privacy Challenges in Cloud Computing

Cloud computing is a widely well-discussed topic today with interest from all fields, be it research, academia, or the IT industry. It has seen suddenly started to be a hot topic in international conferences and other opportunities throughout the whole world. The spike in job opportunities is attributed to huge amounts of data being processed and stored on the servers. The cloud paradigm revolves around convenience and easy the provision of a huge pool of shared computing resources.

The rapid development of the cloud has led to more flexibility, cost-cutting, and scalability of products but also faces an enormous amount of privacy and security challenges. Since it is a relatively new concept and is evolving day by day, there are undiscovered security issues that creep up and need to be taken care of as soon as discovered. Here we discuss the top 7 privacy challenges encountered in cloud computing:

1. Data Confidentiality Issues

Confidentiality of the user's data is an important issue to be considered when externalizing and outsourcing extremely delicate and sensitive data to the cloud service provider. Personal data should be made unreachable to users who do not have proper authorization to access it and one way of making sure that confidentiality is by the usage of severe access control policies and regulations. The lack of trust between the users and cloud service providers or the cloud database service provider regarding the data is a major security concern and holds back a lot of people from using cloud services.

2. Data Loss Issues

Data loss or data theft is one of the major security challenges that the cloud providers face. If a cloud vendor has reported data loss or data theft of critical or sensitive material data in the past, more than sixty percent of the users would decline to use the cloud services provided by the vendor. Outages of the cloud services are very frequently visible even from firms such as Dropbox, Microsoft, Amazon, etc., which in turn results in an absence of trust in these services during a critical time. Also, it is quite easy for an attacker to gain access to multiple storage units even if a single one is compromised.

3. Geographical Data Storage Issues

Since the cloud infrastructure is distributed across different geographical locations spread throughout the world, it is often possible that the user's data is stored in a location that is out of the legal jurisdiction which leads to the user's concerns about the legal accessibility of local law enforcement and regulations on data that is stored out of their region. Moreover, the user fears that local laws can be violated due to the dynamic nature of the cloud makes it very difficult to delegate a specific server that is to be used for trans-border data transmission.

4. Multi-Tenancy Security Issues

Multi-tenancy is a paradigm that follows the concept of sharing computational resources, data storage, applications, and services among different tenants. This is then hosted by the same logical or physical platform at the cloud service provider's premises. While following this approach, the provider can maximize profits but puts the customer at a risk. Attackers can take undue advantage of the multi-residence opportunities and can launch various attacks against their co-tenants which can result in several privacy challenges.

5. Transparency Issues

In cloud computing security, transparency means the willingness of a cloud service provider to reveal different details and characteristics on its security preparedness. Some of these details compromise policies and regulations on security, privacy, and service level. In addition to the willingness and disposition, when calculating transparency, it is important to notice how reachable the security readiness data and information actually are. It will not matter the extent to which the security facts about an organization are at hand if they are not presented in an organized and easily understandable way for cloud service users and auditors, the transparency of the organization can then also be rated relatively small.

6. Hypervisor Related Issues

Virtualization means the logical abstraction of computing resources from physical restrictions and constraints. But this poses new challenges for factors like user authentication, accounting, and authorization. The hypervisor manages multiple Virtual Machines and therefore becomes the target of adversaries. Different from the physical devices that are independent of one another, Virtual Machines in the cloud usually reside in a single physical device that is managed by the same hypervisor. The compromise of the hypervisor will hence put various virtual machines at risk. Moreover, the newness of the hypervisor technology, which includes isolation, security hardening, access control, etc. provides adversaries with new ways to exploit the system.

7. Managerial Issues

There are not only technical aspects of cloud privacy challenges but also non-technical and managerial ones. Even on implementing a technical solution to a problem or a product and not managing it properly is eventually bound to introduce vulnerabilities. Some examples are lack of control, security and privacy management for virtualization, developing comprehensive service level agreements, going through cloud service vendors and user negotiations, etc.

Social Media Marketing: Security Risks and Perils for Organizations

Social media marketing has become dominant in the industry. According to fall 2009 survey by marketing professionals; usage of social media sites by large business-to-business (B2B) organizations shows the following:

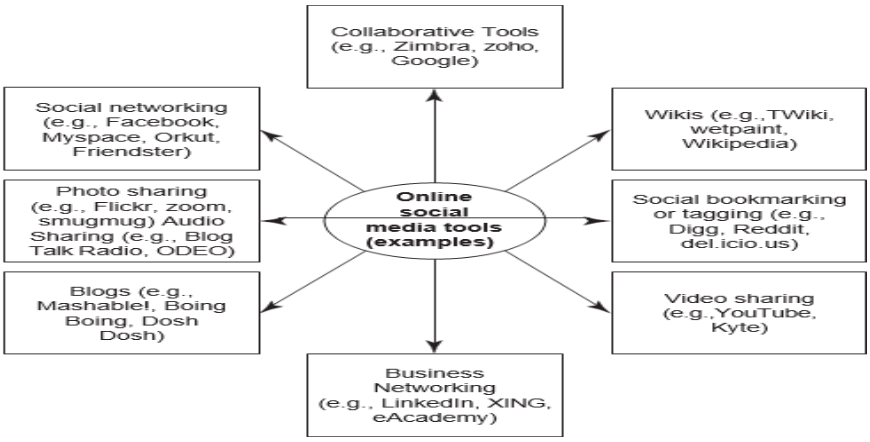

Collaborative Tools (e.g., Zimbra, zoho, Google)
Social networking (e.g., Facebook, Myspace, Orkut, Friendster)
Wikis (e.g.,TWiki, wetpaint, Wikipedia)
Photo sharing (e.g., Flickr, zoom, smugmug) Audio Sharing (e.g., Blog Talk Radio, ODEO)
Online social media tools (examples)
Social bookmarking or tagging (e.g., Digg, Reddit, del.icio.us)
Blogs (e.g., Mashable!, Boing Boing, Dosh Dosh)
Video sharing (e.g.,YouTube, Kyte)
Business Networking (e.g., LinkedIn, XING, eAcademy)

FIG: Social Media Marketing Tools

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

Although the use of social media marketing site is rampant, there is a problem related to "social computing" or "social media marketing" – the problem of privacy threats. Exposures to sensitive PI and confidential business information are possible if due care is not taken by organizations while using the mode of "social media marketing."

- **Understanding Social Media Marketing**

Most professionals today use social technologies for business purposes. Most common usage include: marketing, internal collaboration and learning, customer service and support, sales, human resources, strategic planning, product development.

Following are the most typical reasons why organizations use social media marketing to promote their products and services:

1. To be able to reach to a larger target audience in a more spontaneous and instantaneous manner without paying large advertising fees.
2. To increase traffic to their website coming from other social media websites by using Blogs

and social and business-networking. Companies believe that this, in turn, may increase their "page rank" resulting in increased traffic from leading search engines.

3. To reap other potential revenue benefits and to minimize advertising costs because social media complements other marketing strategies such as a paid advertising campaign.
4. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
5. To collect potential customer profiles. Social media sites have information such asuser profile data, which can be used to target a specific set of users for advertising

There are other tools too that organizations use; industry practices indicate the following:

1. Twitter is used with higher priority to reach out to maximum marketers in the technology space and monitor the space.
2. Professional networking tool LinkedIn is used to connect with and create a communityof top executives from the Fortune 500.
3. Facebook as the social group or social community tool is used to drive more traffic to Websense website and increase awareness about Websense.
4. YouTube (the video capability tool to run demonstrations of products/services, etc.) is used to increase the brand awareness and create a presence for corporate videos.
5. Wikipedia is also used for brand building and driving traffic.

There are conflits views about social media marketing some people in IT say the expensive and careless use of it.Some illustrate the advantages of it with proper control of Security risk

What is social media security?

Social media security refers to strategies businesses and individuals can use to **protect their social accounts from threats like hacking, phishing, and malware**.

The most common social media security risks

In this section, we cover:

- Phishing attacks and scams
- Imposter accounts
- Malware attacks and hacks
- Vulnerable third-party apps
- Password theft
- Privacy settings and data security
- Unsecured mobile devices

Phishing attacks and scams

Phishing scams are some of the most common social media cyber security risks. In a phishing scam, the goal is to **get you or your employees to hand over passwords, banking details, or other sensitive information**.

One common phishing scam involves fake coupons for big-name brands like Costco, Starbucks, and Bath & Body Works. This is especially popular on Facebook. To claim the coupon, you have to hand over personal information like your address and birth date.

Some scammers are bolder, asking for banking information and passwords for a coupon processing fee.

Romance scams are another common social media security problem: 40% of those who fall victim to this type of scam say it started on social media. The FTC reports that for users aged 18-29, sextortion scams originating on Instagram and Snapchat were of particular concern in 2022.

For Americans aged 20 to 39, social media is the most common contact method for scammers.

Imposter accounts

It's relatively easy for an imposter to create a social media account that looks like it belongs to your company. This is one reason why it's so valuable to get verified on social networks.

LinkedIn's latest transparency report notes that they took action on 21.9 million fake accounts in just six months. The majority of those accounts (95.3%) were blocked automatically at registration. But more than 190,000 fake accounts were only addressed once members reported them.

Meanwhile, Facebook took action on 1.3 billion fake accounts between October and December 2022. The social media platform estimates that 4-5% of monthly active users are fake accounts.

Impostor accounts can target your customers, employees, or prospective hires. When your connections are tricked into handing over confidential information, it's your reputation that suffers. Imposter accounts may also try to con employees into handing over login credentials for corporate systems.

Another type of imposter scam targets brands hoping to work with influencers. In this scam, someone impersonating a social media personality with a high following reaches out and asks for free product.

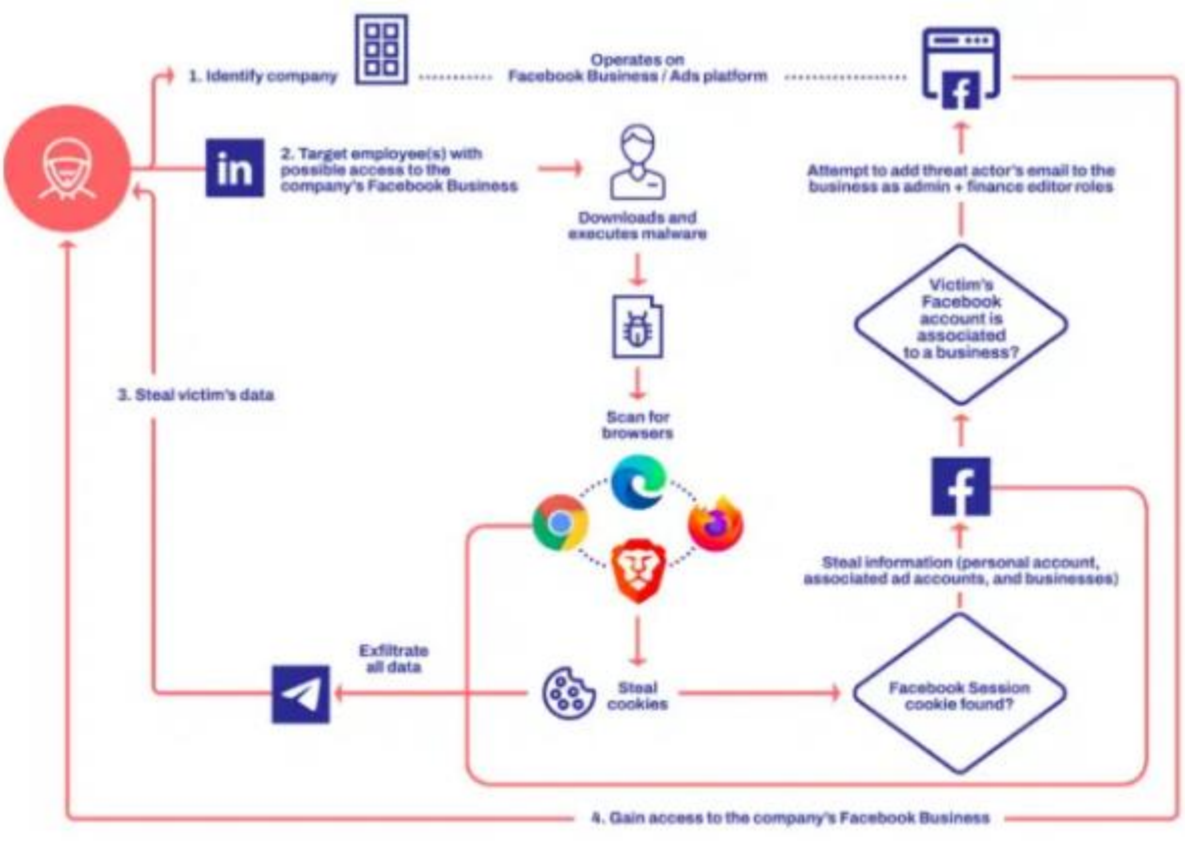
Working with real influencers can be a valuable marketing strategy. But it's important to verify that you're dealing with the real person.

Malware attacks and hacks

In one of the more embarrassing recent social media cyber security incidents, the personal Twitter account of the U.S. Ambassador at Large for Cyberspace & Digital Policy was hacked in February:

If hackers gain access to your social media accounts, they can cause **enormous brand reputation damage**. If they manage to install malware, there is even greater risk.

In 2022, the “Ducktail” campaign was found to target employees on LinkedIn, then convince them to open an attachment containing malware. The malware used browser cookies to hijack the target’s Facebook Business accounts.


1. Identify company
Operates on Facebook Business / Ads platform
2. Target employee(s) with possible access to the company's Facebook Business
Downloads and executes malware
Attempt to add threat actor's email to the business as admin + finance editor roles
Victim's Facebook account is associated to a business?
3. Steal victim's data
Scan for browsers
Steal information (personal account, associated ad accounts, and businesses)
Exfiltrate all data
Steal cookies
Facebook Session cookie found?
4. Gain access to the company's Facebook Business

Vulnerable third-party apps

Locking down your own social accounts is great. But hackers may still be able to **gain access to your secure social media through vulnerabilities in connected third-party apps**

Instagram specifically warns about third-party apps that claim to provide likes or followers:

“If you give these apps your login information, whether with an access token or by giving them your username and password, they can gain complete access to your account. They can see your personal messages, find information about your friends, and potentially post spam or other harmful content on your profile. This puts your security, and the security of your friends, at risk.”

Password theft

Those social media quizzes that ask about your first car might seem like harmless fun. But online social media challenges and quizzes are a common method for **gathering password information or gaining personal details** that are often used as forgotten password clues.

By completing them, employees can accidentally create social media security issues.

Privacy settings and data security

People seem to be well aware of the potential privacy risks of using social media. Overall trust in social networks' ability to protect privacy and data has been shrinking in recent years. In particular, TikTok has recently been in the news as governments around the world restrict access to the platform on official equipment based on data security concerns.

Those concerns, of course, don't stop people from using their favorite social channels. The number of active social media users grew 4.2% in 2022 to 4.74 billion people.

Make sure you – and your team – understand the privacy policies and settings for both your personal and business accounts. You should provide privacy guidelines for employees who use their personal social accounts at work.

Unsecured mobile phones

Mobile devices account for more than half the time we spend online. Social media apps make it easy to access your social media accounts with just one tap.

That's great as long as your phone stays in your own hands. But if your phone, or an employee's phone, is lost or stolen, one-tap access makes it easy for a thief to access social accounts. Then they can **post to your account, or even message your connections with phishing or malware attacks**.

Protecting the device with a password, fingerprint, or face verification helps, but a surprising number of mobile users still leave their phones unlocked.

8 social media security best practices for 2023

1. Create a social media policy

A social media policy is a set of guidelines that outline how your business and your employees should use social media responsibly.

This will help protect you not only from social media and cyber security threats, but from bad PR or legal trouble as well.

At minimum, the security section of your social media policy should include:

- Rules related to personal social media use on business equipment
- Social media activities to avoid, like quizzes that ask for personal information
- Which departments or team members are responsible for each social media account
- Guidelines on how to create an effective password and how often to change passwords
- Expectations for keeping software and devices updated
- How to identify and avoid scams, attacks, and other security threats
- Who to notify and how to respond if a social media security concern arises

For more details, check out our step-by-step guide to creating a social media policy. It includes loads of examples from different industries.

2. Require two-factor authentication

Two-factor authentication is not foolproof, but it does provide a powerful extra layer of security for your social media accounts. You don't have to take our word for how important this is – Instagram head Adam Mosseri reminds his followers every month.

3. Train your staff on social media security awareness

Even the best social media policy won't protect your organization if your employees don't follow it. Of course, your policy should be easy to understand. But training will give employees the chance to engage, ask questions, and get a sense of how important it is to follow.

These training sessions are also an opportunity to review the latest threats on social. You can talk about whether there are any sections of the policy that need updating.

It's not all doom and gloom. Social media training also equips your team to use social tools effectively. When employees understand best practices, they feel confident using social media for their work. They're then well-equipped to use social media safely for both personal and professional purposes.

4. Limit access to increase social media data security

Limiting access to your social accounts is the best way to keep them secure. You might be focused on threats coming from outside your organization. But employees are a significant source of data breaches.

You may have whole teams of people working on social media messaging, post creation, or customer service. But that certainly doesn't mean that everyone needs to know the passwords to your social accounts.

It's critical to have a system in place that allows you to revoke access to accounts when someone leaves your organization or changes roles. Learn more about how this works in the Tools section below.

5. Set up a system of approvals for social posts

Not everyone who works on your social accounts needs the ability to post. It’s an important defensive strategy to limit the number of people who can post on your accounts. Think carefully about who needs posting ability and why.

You can use Hootsuite to give employees or contractors the ability to draft messages. Then, they’re all set to post at the press of a button. Leave that last button press to a trusted person on your team.

6. Put someone in charge

Assigning a key person as the eyes and ears of your social presence can go a long way towards mitigating risks. This person should:

- own your social media policy
- monitor your brand’s social presence
- determine who has publishing access
- be a key player in the development of your social media marketing strategy

This person will likely be a senior player on your marketing team. But they should maintain a good relationship with your company’s IT department to ensure marketing and IT work together to mitigate risk.

This is the person team members should turn to if they ever make a mistake on social that might expose the company to risk of any kind. This way the company can initiate the appropriate response.

7. Set up an early warning system with social media security monitoring tools

Keep an eye on all of your social channels. That includes the ones you use every day as well as the ones you’ve registered but never used at all.

Assign someone to check that all the posts on your accounts are legitimate. Cross-referencing your posts against your content calendar is a great place to start.

Follow up on anything unexpected. Even if a post seems legitimate, it’s worth digging into if it strays from your content plan. It may be simple human error. Or, it may be a sign that someone has gained access to your accounts and is testing the water before posting something more malicious.

Use your social media monitoring plan to watch for:

- imposter accounts
- inappropriate mentions of your brand by employees
- inappropriate mentions of your brand by anyone else associated with the company

- negative conversations about your brand

You can learn how to monitor all the conversations and accounts relevant to your brand in our complete guide to social media listening. And check out the Tools section below for information on resources that can help.

8. Regularly check for new social media security issues

Social media security threats are constantly changing. Hackers are always coming up with new strategies, and new scams and viruses can emerge at any time.

Regular audits of your social media security measures will help keep you ahead of the bad actors.

At least once a quarter, be sure to review:

- **Social network privacy settings.** Social media companies routinely update their privacy settings. This can impact your account. For example, a social network might update its privacy settings to give you more precise control over how your data is used.
- **Access and publishing privileges.** Check who has access to your social media management platform and social accounts. Update as needed. Make sure all former employees have had their access revoked. Check for anyone who's changed roles and no longer needs the same level of access.
- **Recent social media security threats.** Maintain a good relationship with your company's IT team to improve your social media security awareness. They can keep you informed of any new social media security risks. And keep an eye on the news—big hacks and major new threats will be reported in mainstream news outlets.
- **Your social media policy.** This policy should evolve over time. As new networks gain popularity, security best practices change and new threats emerge. A quarterly review will make sure this document remains useful and helps to keep your social accounts safe.

3 social media security tools that will keep your accounts safe

No matter how close an eye you keep on your social channels, you can't monitor them 24 hours a day—but software can. Here are some of our favorite social media security tools.

1. Hootsuite

With a social media management platform like Hootsuite, team members never need to know the login information for any social network account. You can control access and permission, so each person gets only the access they need.

If someone leaves the company, you can disable their account without having to change all your social media passwords.

Hootsuite is also an effective social monitoring tool that keeps you ahead of threats. By monitoring social networks for mentions of your brand and keywords, you'll know right away when suspicious conversations about your brand emerge.

Say people are sharing phony coupons, or an imposter account starts tweeting in your name. You'll see that activity in your streams and can take action before your customers get scammed.

Hootsuite is also FedRamp authorized and Cyber Essentials compliant. Learn more about our risk management program and information security policies.

2. ZeroFOX

ZeroFOX is a cybersecurity platform that provides automated alerts of:

- dangerous, threatening, or offensive social content targeting your brand
- malicious links posted on your social accounts
- scams targeting your business and customers
- fraudulent accounts impersonating your brand

It also helps protect against hacking and phishing attacks.

3. BrandFort

BrandFort can help protect your social accounts from spam and phishing comments and other content moderation issues.

Why are spam comments a security risk? They're visible on your profiles and may entice legitimate followers or employees to click through to scam sites. You'll have to deal with the fallout, even though you did not directly share the spam.

BrandFort can detect spam comments in multiple languages and hide them automatically.

Social media security FAQs

What are the top 5 security threats of social media?

The top 5 social media security threats are:

1. Phishing attacks and scams
2. Imposter accounts
3. Malware attacks and hacks
4. Vulnerable third-party apps
5. Password theft

How do you ensure security on social media?

The best ways to improve security on social media are to limit account access and use two-factor authentication.

Hootsuite's permissions, security, and archiving tools will ensure the safety of all your social profiles—from a single dashboard. See it in action today.

Cyber Security - Organizational Implications

Personal Identifiable Information (PII)

PII is any data that could potentially use to identify a particular person. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual

For an example, PII is an individual's first name or first initial and last name in combination with any of the following data:

1. Aadhaar Number (UID) / Social Security Number (SSN).
2. Driver's license number or identification card number.
3. Bank account number, credit or debit card number
4. Home address or E-Mail address.

Insider Threat

It is defined as "the misuse or destruction of confidential information as well as IT equipment by employees, contractors and other 'trusted' individuals".

Three types of "insiders":

1. **Malicious insider** : is motivated to adversely impact an organization that compromise information confidentiality or integrity.
2. **Careless insider :** shares the information not by any bad intention but simply by being careless due to an accident, mistake or negligence.
3. **Tricked insider** : is a person who is "tricked" to provide sensitive data by people who are not truthful about their identity or purpose through known as social engineering.

Privacy

Cybercrimes take place due to weakness of cyber security practices and "privacy". Privacy has following four key dimensions:

1. Informational/data privacy
2. Personal privacy
3. Communication privacy
4. Territorial privacy

Challenges from emerging new information threats to organizations

The key challenges from emerging new information threats to organizations are as follows:

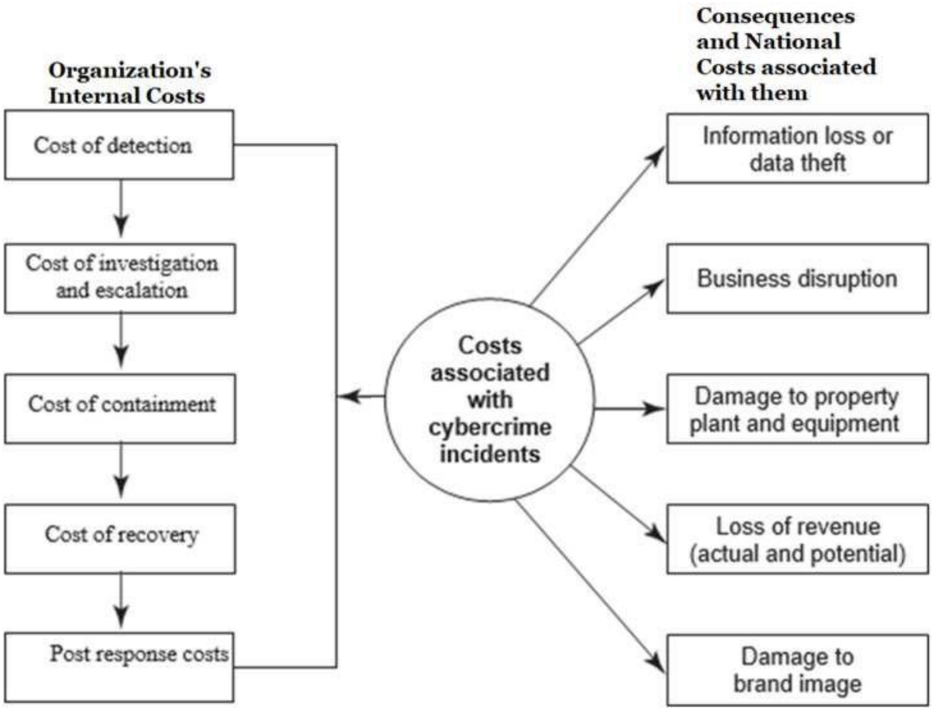
1. Industrial espionage: There are several tools available for web administrators to monitor and track the various pagesand objects that are accessed on their website.

2. **IP-based blocking:** This process is often used for blocking the access of specific IP addresses and/or domain names.
3. **IP-based cloaking:** It is the process of a web server delivering a specific web page based on the visitor's IP address.
4. **Cyberterrorism:** Refers to the direct intervention of a threat source towards organization's website.
5. **Confidential information leakage:** Attacks by the insider or outsider.

Cost of Cybercrimes and IPR Issues: Lessons for

OrganizationsCost associated with Cybercrimes

- When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations andthere are organizational impacts as well.
- Detection and recovery constitute a very large percentage of internal costs.


Organization's Internal Costs
Cost of detection
Cost of investigation and escalation
Cost of containment
Cost of recovery
Post response costs
Costs associated with cybercrime incidents
Consequences and National Costs associated with them
Information loss or data theft
Business disruption
Damage to property plant and equipment
Loss of revenue (actual and potential)
Damage to brand image

Organization's Internal Costs:

The internal costs typically involve people costs, operating costs and productivity losses.

1. Cost of detection
2. Cost of investigation and escalation
3. Cost of containment (control or suppression)
4. Cost of recovery
5. Post response cost

Consequences and National Cost Associated with them:

1. Information loss or data theft
2. Business disruption
3. Damage to property and equipment
4. Loss of revenue
5. Damage to brand image of the organization

Web Threats for Organizations: The Evils and Perils

- The Internet and web is the way of working in today’s interconnected digital world.
- Large number of companies as well as individuals has a connection to the Internet.
- IT managers must find a balance between allowing reasonable personal Internet use at work and maintainingoffice work productivity.

Overview of Web Threats to Organizations

The following are the Internet and Web Threats to Organizations:

- Employee wasting time on social networking sites and its impact on employee productivity.
- Monitoring and Controlling Employees’ web usage.
- Keeping security systems with up-to-date patches.
- Legal and regulatory compliance risks such as employee visiting inappropriate websites and accidental disclosure of information.
- Keeping internet bandwidth free for applications such as live video conferencing, YouTube, and online trainingvideos.
- Monitoring cell phones/smart phones usage and security threats imposed by handheld devices.
- Protecting multiple offices and locations because of globalization.

Social Media Marketing: Security Risks for Organizations

- Social media marketing has become dominant in the industry and is used extensively.
- There are security problem (privacy threats) related to “social media marketing” or “social computing”.
- Exposures to sensitive PII and confidential business information are possible if due care is not taken by organizations.

According to a survey, usage of social media sites by large business-to-business (B2B) organizations shows the following:

1. Facebook is used by 37% of the organizations.
2. LinkedIn is used by 36% of the organizations.
3. Twitter is used by 36% of the organizations.
4. YouTube is used by 22% of the organizations.
5. My Space is used by 6% of the organizations.

Understanding Social Media Marketing

Following are the most typical reasons why organizations use social media marketing to promote their products andservices:

1. To be able to reach to a larger audience in an instant manner.
2. To increase traffic to their website coming from other social media websites.
3. Companies believe that this may increase their “page rank” resulting in increased traffic from leading searchengines.
4. To minimize advertising costs.

5. To build credibility by participating in relevant product promotion forums and responding to potential customers' questions immediately.
6. To collect customer profiles. Social media sites have information such as user profile data, which can be used totarget a specific set of customers for advertising.

Organizational Implications of Software Piracy

Use of pirated software is a major risk area for organizations.

1. From a legal point of view, software piracy is an IPR violation crime.
2. Use of pirated software increases risks of cybercrime and computer security.

Security and Privacy Implications from Cloud Computing

There are data privacy risks associated with cloud computing.
Three kinds of spheres and their characteristics which are associated with cloud computing are as follows:

1. User sphere:
Here data is stored on user's computer, mobile phones, Radio Frequency Identification (RFID) chips, etc. Organization's responsibility is to provide access to legitimate users and ensure misuse does not happen.

2. Recipient sphere:
Here, data lies with recipients. That is servers and databases of cloud computing service providers or other third partieswith whom data recipient shares data.

3. Joint sphere:
Here data lies with web service provider's servers and user's servers. This is also called in-between sphere.

Social Computing and the Associated Challenges for Organizations

- Social computing is also known as "Web 2.0" which empowers people to use Web-based public products andservice.
- Social computing is directly related to the social media marketing.
- Social computing helps people across the globe to support their work, learning, and get entertained.
- In this process information gets exchanged and it may contain PII or confidential information of the organization.
- This information would be a gold mine for cyber criminals.

Protecting People's Privacy in the Organization

- Tracking and monitoring people on the Internet is a controversial issue.
- From privacy perspective, people would hate to be monitored in terms of what they are doing, what they aremoving, etc.

Organizational Guidelines for Internet Usage

Appropriate Internet Usage by Employee

Employees are advised to use organization's internet connection for the following reasons:

1. To complete their job duties.

2. To seek out information that they can use to improve their work.
3. To access their social media accounts, while conforming to social media policy and privacy
4. Employees should:
   - Log into their corporate accounts only from safe devices.
   - Use strong passwords to log into work-related websites and services.
   - Keep their passwords confidential at all times.

Inappropriate Internet Usage by Employee

Employees **mustn't** use organization's internet connection for the following reasons:

1. Download or upload obscene, offensive or illegal material.
2. Send confidential information to unauthorized recipients.
3. Invade (assault) another person's privacy and sensitive information.
4. Download or upload copyrighted software and other digital data such as movies and music.
5. Perform unauthorized or illegal actions, like hacking, fraud, buying/selling illegal goods.

Safe Computing Guidelines and Computer Usage Policy

1. Install anti-virus software
2. Keep Operating System up to date
3. Take a back-up
4. Use a secure password
5. Use a desktop firewall
6. Keep programs up-to-date with the latest patches
7. Physically secure your computer
8. Log out when you don't use
9. Don't store sensitive data on your computer
10. Exercise Internet and email safety

Incident Handling: An Essential Component of Cyber security

Computer security incident means "any adverse event which compromises some aspects of computer or computernetwork security".

Classification of incidents:

- IT security incidents
- Data incidents / Data privacy incidents
  - Any loss/theft of organizational confidential data or client information

IT Incidents

Following are the types of IT security incidents:

- Inappropriate usage of organization's assets/resources
- Tampering with IT controls such as disabling firewall, stopping antivirus software, etc
- Unauthorized changes to IT systems
- Spam and email forgery
- Use of unlicensed software / tools / applications
- Downloading inappropriate materials
- DoS that affects services to legitimate users

Priorities of Incidents

Incidents are prioritized as follows:

1. **High priority incidents**
   These have high impact on the organization's business or service to customer.
   Incident response team must respond immediately.
   Ex: Malicious code attacks including Trojan horse program, Virus infections and unauthorized system access

2. **Medium priority incidents**
   These have significantly moderate impact on organization's business or service to customers.
   Incident response team can respond using standard procedures within normal management structures.Ex: Password cracking attempts.

3. **Low priority incidents**
   These have low impact on the organization's business or services to customer.
   Incident response team can respond using standard procedures when time allows.Ex: Denial access to the system due to unexpected lockout.

CYBER SECURITY: ORGANIZATIONAL IMPLICATIONS

Do you how much is lost in cybercrime annually?
It is estimated that at least $600, 000, 000, 000 is drained out of the global economy annually only through Cybercrime. And do you how much it costs an attacker to conduct a cyber heist.? In this article, we will be looking at what cybersecurity for an organization means and what actions they take to protect themselves from cyber-attacks.

CyberSecurity in Organizations

Computer security or cybersecurity is protecting oneself or an organization from malicious attacks for monetary or other indirect gains. With a lot of knowledge and resources available at hand on demand (on the Internet), it's become quite common that even someone who has a basic idea of how to google can cause a ruckus. An individual or organization needs to be secure digitally as they are physically. Organizations tend to maintain their security teams or hire a trusted third party that is capable of.
Cybersecurity teams have become an integral part of most organizations. When we consider cybersecurity teams, in general, they focus towards the centralized issues that are on the organizations' priority list, like data, applications, cloud, network services, etc. Companies usually have an infrastructure team, a threat management team and Identity and access management (IAM) team. Not all the organizations need to have the same structure or the same names, this is just an overview of how they work. The infrastructure is a very important asset of an organization and so it must be protected. The infrastructure security team are responsible for managing the audits, risks, disaster recovery programs and compliance of the infrastructure with market standards. Most common security standards are ISO 27001 and PCI-DSS.
The threat team is responsible for testing an application for vulnerabilities and report them for avoiding any exploits. The SOC team, which most of the times come under threat management team, is responsible for blocking and monitoring real-time attacks. You might have seen this many times in movie or some other places, the place where there will be a lot of huge screens are put displaying things (Yes, they do exist and many large organizations do this to keep an eye over their network. While all these teams seem familiar the IAM team is not known by many, this team is responsible for

identifying a user and manage access to the resources as required. Interestingly the market for IAM tools is gaining as IAM is at the endpoint of security, i.e., the users(employees in the organization). Tools like cyberark, Sailpoint, okta, BeyondTrust and oracle identity management are the top tools used by most organizations to tighten their security while not causing and dent in their workflow.

Current State of Security:

So from the structure of the security teams, we can see that organizations have started considering every aspect of the environment to protect themselves from cyber-attacks. Attacking on an organization (small to large) can cost somewhere around $112, 000 to anywhere up to $3.8 million and over, depending on the type of attack and what their intentions are.

Statistics say that margin between the cost of attack and the gain from attacks have started to reduce (Obviously leaving aside the social aspects of an attacker) as more and more organizations have invested in cybersecurity as the value of the information they hold is also risen dramatically.

What Organizations Need to Know about Cyber Security?

Cyber security or IT security is the protection of computer systems and networks from information disclosure, theft or damage of their hardware, software or electronic data, as well as the disruption or misdirection of the services they provide.

Cyber security aims to eliminate the risk of cyber-attacks and guard the system, networks, data and devices from unauthorized, unwarranted exploitation.

Legal requirement for cyber security

Yes, it is crucial for the organization to have cyber security measures in place. The GDPR (General Data Protection Regulation) and DPA (Data Protection Act) 2018 require organizations to implement fitting security measures to protect personal data.

Importance of cyber security

The rationale and benefits of cyber security are detailed as follows:

1. Increasingly sophisticated cyber-attacks are coming up. The tactics and the reach of cyber attackers are ever-increasing, including malware and ransomware, phishing, social engineering, insider threats, advanced persistent threats and others.
2. Unauthorized user access is prevented. Cyber security addresses vulnerabilities of the system and the network, thereby securing it from unauthorized access.
3. End users and devices are protected. Data privacy is maintained by the upkeep of cyber security. Data and network protection is also ensured.
4. Regulations are increasing the costs of cyber security breaches. Hefty fines are imposed by privacy laws like the GDPR and DPA on organizations that ignore the threat of cyber attacks.
5. Cyber security ensures the continuity of the business which is critical to the success of any organization.
6. Cyber security measures translate into a rise in the reputation of the company and consequently improved trust in the relationship with its clientele and all the stakeholders.

Types of Cyber-attacks

Cyber security risks can be even more challenging if the organization has resorted to remote working and hence has less control over employees’ activities and device security. A cyber attack can cost organizations billions and severely damage its reputation. Those organizations will likely lose sensitive data and face huge fines.

The different types of cyber-attacks include:

- **Malware**: It is a kind of malicious software that can use any file or software to harm a computer user, such as worms, viruses, Trojans and spyware.

- **Social engineering**: Users are tricked into breaking security procedures and the attackers gain sensitive, protected information.
- **Phishing**: Fraudulent emails and text messages resembling those from reputable sources are sent at random to steal sensitive information such as credit cards.
- **Spear Phishing**: It is a form of phishing attack but it has a particular (intended) target user or organization.
- **Ransomware**: It is another type of malware in which the system is locked by an attacker through encryption that they would not decrypt and unlock until the ransom is paid.

Other common attacks include insider threats, distributed denial of service, advanced persistent threats, man-in-the-middle attacks, botnets, vishing, business email compromise, SQL injection attacks and zero-day exploits.

Effective training of the employees will enable them to understand the significance of cyber security. Regular cyber security risk assessment to evaluate risks and checking if the existing security controls are appropriate and if not, making mid-course corrections, will protect the company from cyber-attacks.

Automation and cyber security

The ever-increasing sophistication in cyber threats has led to automation becoming an integral component of cyber protection. Machine learning and Artificial Intelligence (AI) help in threat detection, threat response, attack classification, malware classification, traffic analysis, compliance analysis and more.

ITGovernance.co.uk presents a cyber security checklist.

1. **Awareness training for the staff**: Effective training of the employees and knowledge sharing of best practices with the employees about the threats they face is a necessary step in preventing cyber security breaches.
2. **Added focus on web applications security**: Web applications are particularly vulnerable to security breaches: hence it is crucial to increase focus on web application security.
3. **Network security**: It refers to the protection of the integrity and usability of the network and data. A network penetration test helps assess the network for security issues.
4. **Leadership commitment**: This is a very important factor for cyber security: the top management should be involved in and committed to cyber security and invest appropriately.
5. **Strong passwords**: The employees should be trained to create and maintain strong passwords.

Cyber security vendors, tools and services

TechTarget points out cyber security vendors who offer a variety of security tools and services.

- Identity and access management (IAM)
- Firewalls
- Endpoint protection
- Antimalware
- Intrusion prevention/detection systems (IPS/IDS)
- Data loss prevention (DLP)
- Endpoint detection and response
- Security information and event management (SIEM)
- Encryption tools
- Vulnerability scanners
- Virtual private networks (VPNs)
- Cloud workload protection platform (CWPP)
- Cloud access security broker (CASB)

Some of the career opportunities in cyber security include Chief Information Security Officer, Chief security officer, security engineers, security analysts, security architects, penetration testers (ethical hackers), data protection officers, cryptographers and threat hunters.

Cyber security at Hurix – Best Practices

A recent study has shown that there are Cyber Attacks every 39 seconds, and most of them are targeted toward Web applications. So let's talk about some of the best practices we follow at Hurix Digital for protecting your Web application against these common attacks.

1. Input validation means checking user-submitted variables for malicious or erroneous input that can cause strange behaviour. One approach is to implement a whitelist, which contains a set of patterns or criteria that match benign input. The whitelist approach allows conditions to be met and blocks everything.

2. Single Sign-on: It is common to see Web applications that utilize single sign on authentication, which pulls a user's credential from a directory or identity database service. Though convenient, multi-factor authentication can make your application more secure by adding additional authentication steps for authorization. We believe that granularity lease, privilege, and separation of duty should be applied to users in order to prevent access to confidential or restricted data. Applications should run under non-privileged service accounts, and user access to system-level resources should be restricted. We have all seen information error messages that range from simple built-in notes to full-blown debugging information.

3. Application errors: should never reveal sensitive application implementation or even configuration settings, as this can be exploited by an attacker. So we keep those error messages generic. Storing secrets in a plain text password is also a big No. Information should never be stored in a publicly accessible location, such as a web directory or repository. We utilize the strongest encryption protocols and algorithms that meet compliance requirements.

4. Code reviews during the development and testing stages should always be done to provide code coverage and ensure secure code practices are utilized. Application scanning can help identify vulnerabilities prior to deployment. Vulnerability and compliance scanning can be done for supporting infrastructure of the application. At HurixDigital, we make sure that the security requirements are baked into our agile design and implementation process. Also, we ensure continuous monitoring and application scanning aligned to meet compliance requirements.

5: Protection from malicious attacks: We implement input validations, anti-forgery tokens, cross-site scripting attacks, brute force attacks, checking sensitive information disclosure and other strong coding practices. Also, continuous monitoring and scanning of the application are used to address vulnerabilities and patches required to maintain security compliance.

6: Insecure Direct Object Reference: IDOR vulnerabilities occur when authorization requirements have not been implemented by the developers to access the application. By changing just an identifier i.e., a rest parameter, user1 can access the information of User2. At HurixDigital, we restrict and enforce authorization between objects and do not allow attackers to enumerate or list the values and test access to other points of data. We use GUID (Globally Unique Identifier) or UUID (Universally Unique Identifier) when referencing between data.

7: Authentication and session management: Vulnerabilities resulting, potentially, in user impersonation, protection and credential strength are also considered.

8: Authorization: It is testing the application's ability to protect against vertical and horizontal privilege escalations.

9. Business logic: Applications are tested keeping in mind business logic.

10. Client-side logic: We use the latest versions of the UI technologies like angularJs, reactJs etc.
11. Malware: We do not expose the internal hardware configuration details as much as possible in the web app and use Known modules which are used worldwide.
12. Port scanning: We keep the unused ports with closed and restricted access so that hackers do not easily hack them.
13. Denial of service attacks: We do not allow continuous hits to the specific APIs (Application Programming Interface) which are sensitive in terms of vulnerabilities or functionalities of the web application.
14. Password strength: It is a measure of a password's efficacy against guessing or brute-force attacks. We follow these guidelines to enhance password strength:

- Use 8 or more characters as a minimum password length.
- Use both lowercase and upper-cases, letters, numbers, and symbols.
- If the user is already using passwords on other websites or systems, then avoid the same passwords.

Cyber Attacks in Organizations: Challenges and Implications

Introduction:

In today's digital age, organizations face a constant threat from cyber attacks that can have severe consequences on their operations, reputation, and financial stability. This newsletter explores the challenges organizations encounter in dealing with cyber attacks and highlights the implications for their security posture.

I. Evolving Threat Landscape:

The rapid advancement of technology has led to a parallel rise in sophisticated cyber threats. Hackers and cybercriminals employ various techniques such as malware, phishing, ransomware, and social engineering to exploit vulnerabilities in organizational systems. The ever-evolving nature of these threats poses a significant challenge for organizations to keep up with the latest security measures.

II. Insider Threats:

One of the most challenging aspects of cyber attacks for organizations is the presence of insider threats. Employees or former employees with malicious intent can compromise sensitive data, sabotage systems, or provide unauthorized access to cybercriminals. Mitigating insider threats requires a delicate balance between trust and security, as organizations must implement robust access controls, monitoring systems, and employee awareness programs.

III. Data Breaches and Privacy Concerns:

Data breaches have become alarmingly common, leading to the exposure of sensitive information and violating user privacy. Organizations must adhere to strict data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union, to safeguard customer data. The financial and reputational damage resulting from data breaches can be significant, necessitating proactive measures to prevent and respond to such incidents.

IV. Resource Constraints:

Many organizations, particularly small and medium-sized enterprises, face resource constraints when it comes to cybersecurity. Limited budgets and lack of skilled personnel make it challenging to implement robust security measures and maintain an effective security posture. Cybersecurity awareness training, regular system updates, and investing in reliable security solutions are crucial but often overlooked due to resource limitations.

V. Rapid Technological Advancements:

The rapid adoption of emerging technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) brings new security challenges for organizations. Integrating these technologies into existing infrastructures without compromising security requires specialized knowledge and expertise. Failure to address these challenges effectively can expose organizations to vulnerabilities and potential cyber attacks.

VI. Incident Response and Recovery:

Cyber attacks can be disruptive, causing operational downtime and financial losses. Organizations need to have well-defined incident response plans in place to minimize the impact of attacks. Incident response teams should be trained and equipped to detect, contain, and recover from security incidents promptly. Regular testing and updating of incident response plans are critical to ensure their effectiveness.

VII. Third-Party Risks:

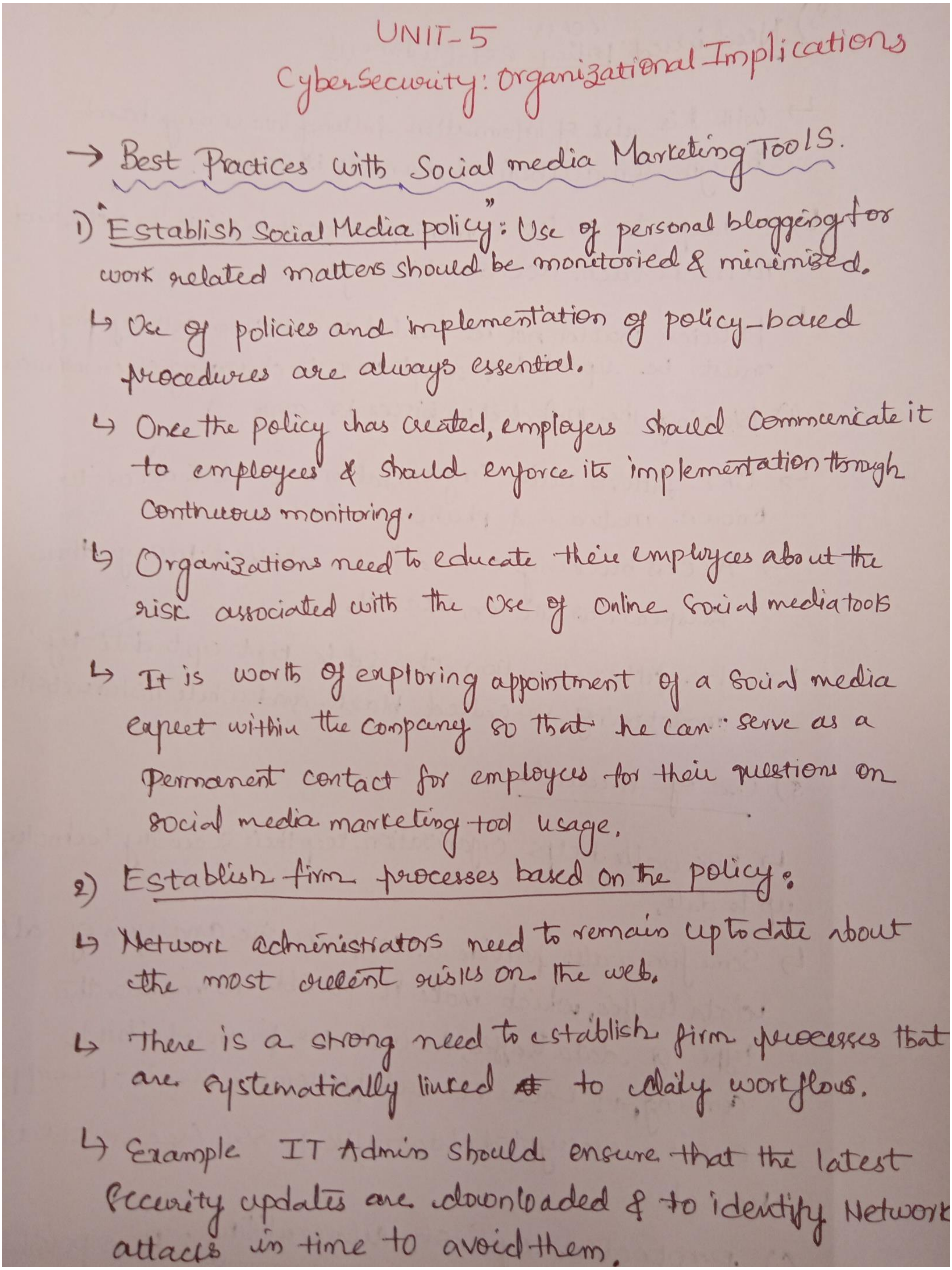
Many organizations rely on third-party vendors and partners for various services and support. However, these relationships can introduce additional risks. Cyber attacks on third-party vendors can compromise organizational systems and data. Organizations must conduct due diligence and establish strong security protocols when engaging with third parties to mitigate these risks.

VIII. Regulatory Compliance:

Organizations are subject to an increasing number of cybersecurity regulations and compliance standards. Failure to comply with these requirements can result in legal repercussions and reputational damage. Navigating the complex landscape of regulatory compliance can be challenging, particularly for multinational organizations operating in different jurisdictions with varying data protection laws.

Conclusion:

Cyber attacks pose significant challenges for organizations across all sectors. To mitigate these threats, organizations must stay vigilant, prioritize cybersecurity measures, and invest in robust infrastructure, personnel training, and incident response capabilities. Proactive risk management, collaboration with security experts, and adherence to regulatory frameworks are essential to safeguard sensitive data and maintain the trust of customers and stakeholders in today's digital landscape.



UNIT-5

CyberSecurity: Organizational Implications

→ Best Practices with Social media Marketing Tools.

1) "Establish Social Media policy": Use of personal blogging for work related matters should be monitoried & minimised.

↳ Use of policies and implementation of policy-based procedures are always essential.

↳ Once the policy has created, employers should communicate it to employees & should enforce its implementation through continuous monitoring.

↳ Organizations need to educate their employees about the risk associated with the use of online social media tools

↳ It is worth of exploring appointment of a social media expert within the company so that he can serve as a permanent contact for employees for their questions on social media marketing tool usage.

2) Establish firm processes based on the policy:

↳ Network administrators need to remain uptodate about the most recent risks on the web.

↳ There is a strong need to establish firm processes that are systematically linked ~~at~~ to daily workflows.

↳ Example IT Admin should ensure that the latest security updates are downloaded & to identify Network attacks in time to avoid them.

3) Need based access policy establishment.

↳ With this risk of information falling into wrong hands through unauthorized channels is reduced.

↳ It helps to control & monitor access to critical data, and to track such access at anytime.

↳ policies should not be treated as one-time activity they must be updated & adapt them to changeing circumstances.

4) Blocking the infected webistes ~~is [illegible]~~

↳ URL filters allow Organizations to block access to known malware & phishing websites.

↳ Access blocking can also be applied to any other suspicious site on Internet.

↳ The filter function should be kept upto date by maintaing so-called black-and white listed websites.

5) Use of firewalls.

↳ Firewalls helps organization keep their security technology up to date,

↳ Some fire walls provide a comprehensive analysis of all data traffic, which make it possible to monitor the type of data traffic, the websites from which it is coming, to know the web patterns & peer to-peer applications to encrypted data traffic in SSL (Secure Socket Layer) tunnel.

6) Protection against vulnerability: It is possible by carefully planning vulnerability scanning & penetration testing.

↳ An Intrusion prevention system (IPS) serves as a protective barrier to the corporate Network by preventing automatically ~~from~~ ~~the~~ attacks by worms viruses & Other malwares.

⑦ <u>Define Access to business Applications</u> : Define need based access to business Applications that reside on Corporate Networks as well as on the external sites.

↳ Example Ex of SSL VPN portal — VPN is Virtual private N/w a tunnel within the internet.

↳ A strong level authentication via Single Sign-On for the User. As a result Single login makes it possible for Users to access Only the Network area & Services for which they are authorized.

⑧ <u>Securing the Intranets</u>: They are not spared by cyberattackers.

↳ Intranet of every Company Consists highly sensitive information pretaining to the business are involved. They should be isolated from rest of internal N/w by using the firewalls to segment the Intranet.

↳ this enables segregation of departmental intranets.

↳ Ex: a company can seperate departments such as finanance or accounting from the rest of the penetrating critical segments of the corporate N/w.

↳ this can be done by DMZ Network (demilititarized Zone Network)

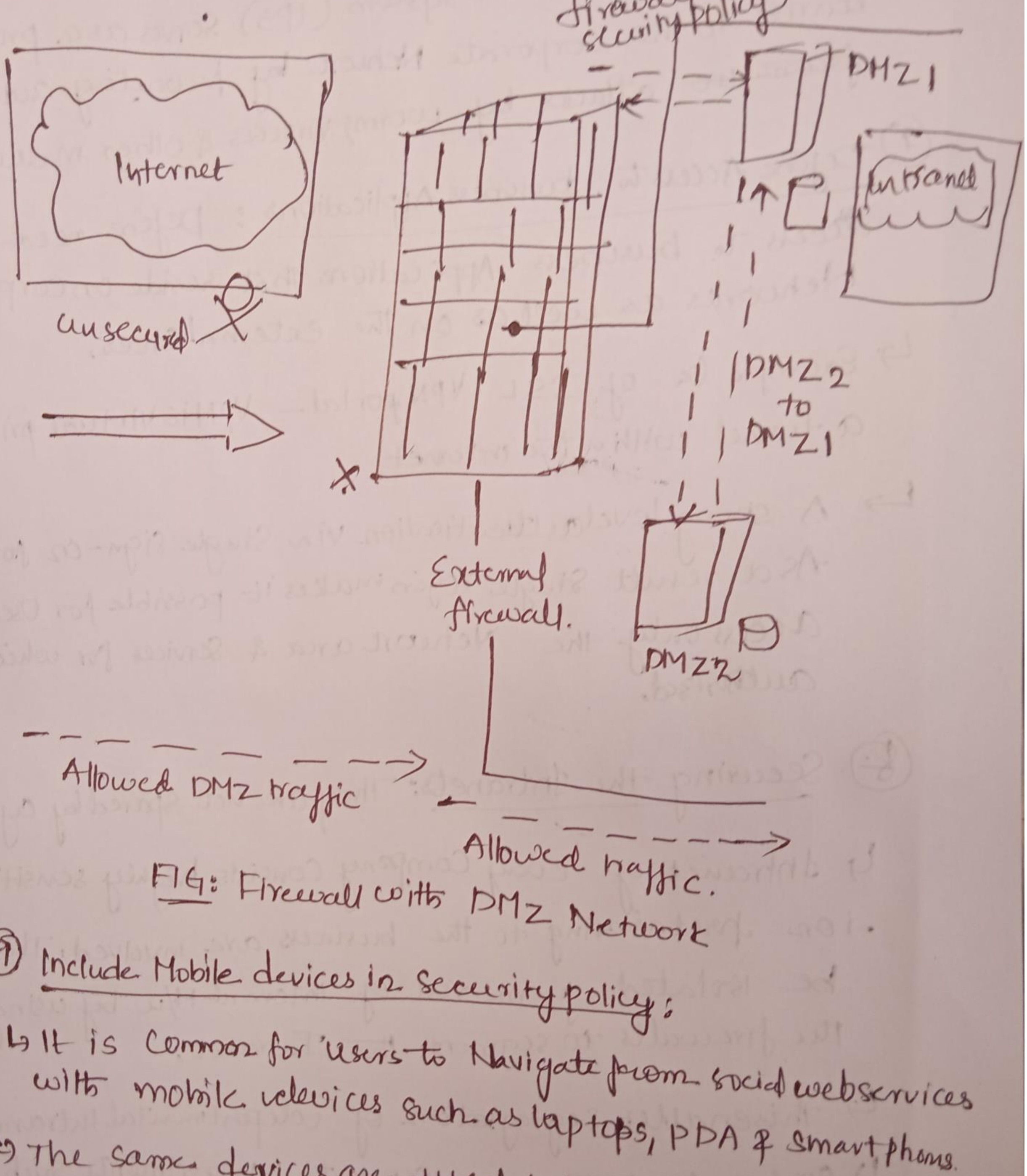


FIG: Firewall with DMZ Network

⑨ Include Mobile devices in security policy:

↳ It is Common for users to Navigate from social webservices with mobile devices such as laptops, PDA & Smart phones.

↳ The same devices are used to log into the Corporate N/w.

↳ The corporate security department, therefore needs to include mobile devices in the securing policies by checking login device for requeied security settings & presence of securing-relevant s/w packages-

(10) Use of Centralized Management: Administrators can manage, monitor and Configure the entire N/w and all devices using a single management Console.

↳ They can also monitor User activities on the N/w by viewing reports.

Ex: ~~N/w~~ System adiminstrator will be able to know who has accessed which data at what time.

↳ this allows preventing attacks more efficiently & provide more protection for corporate Applications at risk.

* Organizational best practices are listed below

1. Organization-wide information system security policy
2. Configuration/Change Control and mangement
3. risk assesment & management
4. Standardized s/w Configurations that Satisfy the information system security policy
5. Security awareness and training
6. Contingency planning, Continuity of operations & disaster recovery Planning.
7. Certification and accrediation

→ Social Computing and The Associated challenges for organizations

- It is also known as "Web 2.0"
- It empowers people to use web based public products and services.
- It helps thousands of people across the globle to support their work, health, learning, getting entert

-aised and citizienship tasks in a number of innovative ways.

↳ In this process, a lot of information gets exchanged & some of that could be Confidential, personally identifiable Information (PII)/SPI etc., This would be gold mine for the cyber Criminals.

↳ Getting too used to readily available information, people may get into the mode of not questioning the accuracy & reliability of information that they readily get on the internet.

↳ with social computing, there are new threats emerging, those threats relate to security, safety & privacy.

* Technical terms *

↳ Various types of mobile workers/remote workers.

1. ~~the~~ Tethered/remote worker: An employee who remains at a single point of work, but is remote to the central company system.

   Ex: Homeworkers, telecottages, branch workers.

2. Roaming user: An employee works in an environment (Eg: warehouses, shopfloor etc.) or in multiple areas (eg: meeting rooms)

3. Nomad: Employees requiring solutions in hotel

modem use is still prevalent, along with wireless technologies & devices

4. Road warrior: This is the ultimate mobile user, such a remote worker spends little time in the office, however he/she requires regular access to data and collaborative functionality while on the move, in transit or in hotels

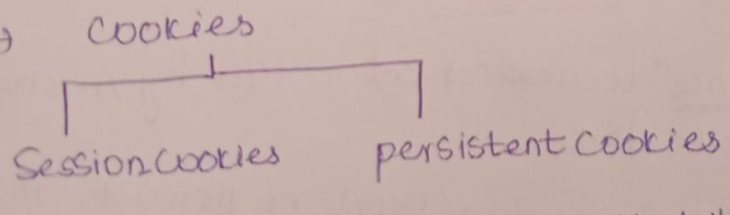
Ex: Sales & field forces.

↳ Cookies

↳ A piece of information that get passed to your browser by a server on the Internet.

↳ They are stored on the hard drvie and are returned to server when requested.

↳



↳ 1) Session cookie is also called "transient cookie" which lasts only for the duration of the internet session.

↳ 2) persistent cookie alsocalled stored cookie

↳ It gets stored on the user's hard drive until it expires or the user deletes the cookie.

↳ In 1994, Netscape created cookies as a Special browser feature. It did so to make Internet browser's life easier while Surfing on the web.

↳ Proactive Vs. Reactive Approach to security

* Proactive approaches are the measures taken with the aim to thwart host-based or N/w based attacks from successfully compromising systems.

↳ This help prevent future business losses.

* Reactive approaches Used after it has been discovered that some of organization's systems have been compromised by an intruder or attack program

↳ Protecting your Online privacy

↳ "Dataveillance" was coined in 1988 by Australian privacy expert clarke.

↳ It is abould monitoring people no through their actions but through data trails about them.

↳ "personal Dataveillance" → Monitoring "identified individuals"

↳ "Mass Dataveillance" → monitoring of whole Population.

↳ The New method browser fingerprinting → to track you online. It can identify far more accurately than Cookie.

↳ It pull data about your browser, plug-in, systemfonts & OS.

Ex: Bank use this to prevent from frauds.

↳ Cookies & fair information practices to Avoid privacy Loss.

↳ IPPs (Information privacy principles) are set out general rules for organization to apply to build the content Use of cookies with regards privacy.

IPP1 — Collection: Manner & ~~pot~~ Purpose of collection of PI

IPP2 — Use & disclosure: Solicitation of PI from individual concerned.

IPP3 — Data quality: Solicitation of PI generally

IPP4 — Data security: Storage & security of PI

IPP5 — Openness: Information relating to records kept by record keeper.

IPP6 — Access & Correction: Access to record Containing PI.

IPP7 — Identifiers: Alteration of records containing PI

IPP8 — Anonymity: Record keep to check accuracy ~~etc.~~ etc. of PI before Use.

IPP9 — Transborder data flows: PI to be used only for relevant purposes.

IPP10 — Sensitive information: limits on use of PI

IPP11 — Limited disclosure: Limits on the disclosure of PI.

———o———o———o———