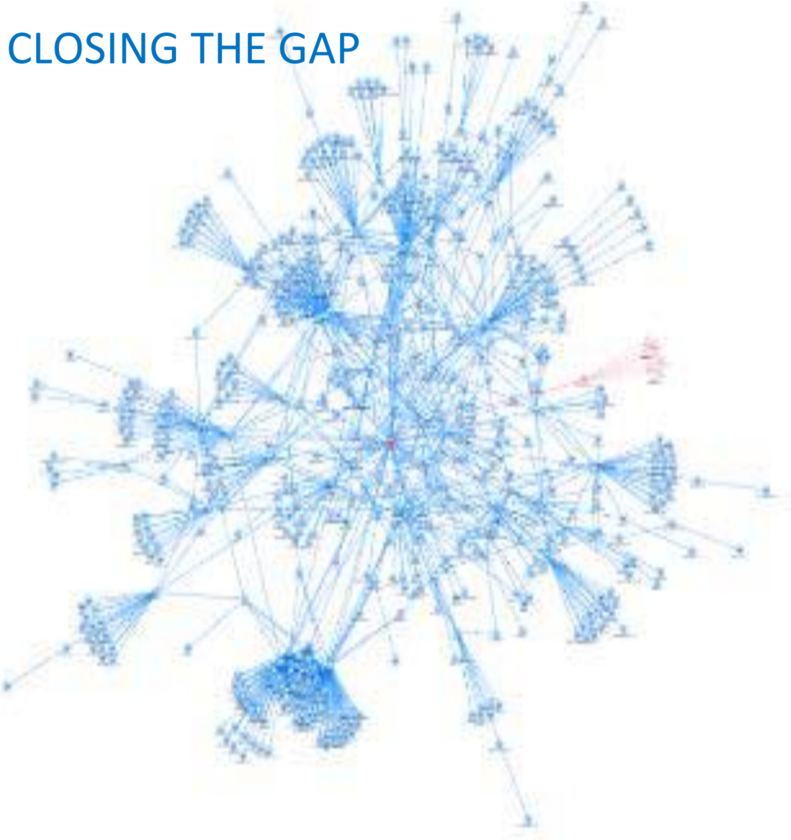
CYBER INSURANCE & RISK MANAGEMENT:

CLOSING THE GAP



Developed by: Lydiah N. Karanja
APA Insurance Ltd, Kenya

The objective of this presentation is to analyze the subject of cyber risk and effective methodologies of mitigating the effects of the said risk exposure. The following are the areas to be covered in this paper:

Description **Page**

1. Definition……………………………………………………………………………………………….2
2. Categories of Cyber Risks…………………………………………………………………………2
3. Sources of Cyber Risks…………………………………………………………………………..2-3
4. Historical Incidences of Cyber Attacks……………………………………………………4-5
5. Why Hackers go unpunished……………………………………………………………………5-6
6. Burden of Cyber Risk……………………………………………………………………………………6
7. Positioning a Company to better manage cyber risks…………………………….7-8
8. Whose responsibility is cyber risk exposure?...5
9. Methods of ensuring cyber security……………………………………………………..8-10
10. Cyber Risk Insurance……………………………………………………………………………11-20
    Coverage
    Extensions
    Exclusions
    Proposal Form
11. Cyber Risk Management…………………………………………………………………...…21-24
    Definition
    Effective Risk Management
    Maintaining Cyber Hygiene
12. Question 1:
    How Your company managed to protect itself against different types of cyber risks………………………………………………………………………………………………..25-28
13. Question 2:
    New products of Cyber Insurance for specific industries (Supply chain, Banks, Petrochemicals, Hotels, etc)……………………………………………………………………29-33
14. Role of the Government enhancing in cyber security……………………………… 35

The insights contained in this research work are purposely intended for this paper and the author's responsibility is limited to this presentation only.

Introduction

It is paramount to first understand the meaning of the word cyber risk to enable us divulge into the insurance and appreciate the risk management aspect of cyber risk.

Cyber Risk can be defined as threat to an organization's digital information as a result of exposure and breach of network security system. Cyber Risk refers to vulnerability of a firm's information systems to fissures or attacks culminating in significant financial loss as well as stained brand reputation.

Cyberspace is a man-made environment created in the U.S. in the late 1960s, based on the developments of post-war technology.

The information system is the heart of any organization in the current era and is useful in running virtually everything about a firm. Right from the company website, storing sensitive medical data on all employees, trade secrets, processing of payroll, emails, telephone connectivity, customers and supplier records as well as online payments; All these are managed by use of the information system. Any threats to such a system will therefore be detrimental to the running of the entire organization by crippling all operations.

Classifying Cyber Risks

Cyber risks can be categorized into two main classifications as expounded hereunder:

- Deliberate Malice. These are intended acts of well-orchestrated attacks by either external hackers or sabotage by irritated employees. This leads to infiltration of network, Denial of Service (DoS) which is unavailability of system for some time, extraction of intellectual property, business interruptions and poor performance of industrial and medical systems.

- Fortuitous Malice. These refer to accidental acts for instance human user error that can render the system temporarily unavailable, natural disasters like hurricanes. A third party whose system is connected could be experiencing system hitches which can spread to the firm's network and cause downtime.

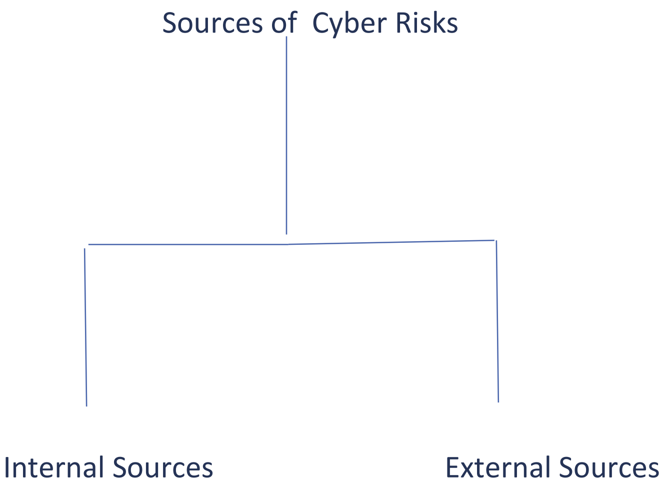
How and Where does Cyber Risk originate from?

There are various sources of cyber risk which will be explained briefly here below.

- Lack of a cyber security policy that identifies threats and unauthorized activities, establishes and develops policies and oversight processes to protect company network and information.

- Mergers and Acquisitions done without conducting a thorough investigation into the target company's cyber history, and its cybersecurity infrastructure and policies.
- The world is a closely knit village as a result of globalization which leads to high threats to the cyber space linking states, corporations and governments.
- Outsourcing of business operations e.g. hired information technology system may pose a great risk to an organization owing to the fact that the supplier may not have a sound cyber security policy in place.
- Adoption of a new technology may pose a major threat in the process of digital migration, cloud integration and connectivity of new devices. During the process of transformation, the firm may find itself in an unfamiliar territory in terms of cyber security. Without clear assessments and interventions hackers will have an easy in through unpatched and outdated solutions, and unforeseen security gaps in newer technologies.
- Extension of third party network and relationships for instance a parent company allowing integration of its network with the subsidiaries and their intermediaries. Such a system tends to be poised for major attacks.
- Allowing a large number of staff to access highly confidential and sensitive company data.

Further, it is worth noting that cyber risks stem from both internal as well as external sources and their impact can be described as either quantitative or qualitative.



- Let’s envision a scenario where a flash disk/laptop containing sensitive data is lost within an organization. The confidential data is stolen/deleted by a disgruntled employee. This leads to a series of hiccups at work ranging from inability to run debtors statements, process invoices, run basic day to day processes in the system, inability to pay suppliers, request for more replenishment of stocks, manage deliveries. This leads to big time downtime and unfortunately reaches the customers who start complaining due to poor customer service. Chances of false statements made on the website or social media are also high which leads to heightened efforts to recover the lost data. Additional cost is incurred and income and profits is lost due to systems downtime. All this time, production has greatly reduced, key employees are being poached by competitors, the market share of the firm has drastically dwindled and all the savings are now being directed towards saving the organization.

- On the external front, a third party can hack into the system and install a virus or disrupt the normal functioning of the system. All the efforts are geared towards saving the organization and at the same time the external environment which includes suppliers, customers, government, community and the media require an explanation on the happenings. All the while, the firm has suffered damage to reputation brand, shareholders start losing confidence in the current management leading to sacking of the CEO , the company starts to record drops in the stock market (if listed), at this point there has to be a profit warning issued, the stakeholders have now exerted extreme pressure on the management to streamline operations, due to loss of confidential data, customers can sue and the firm be penalized for negligence, likelihood of liability claims levelled against the firm are also high emanating from clients whose data is lost. False information spread on the website regarding a claimant could lead to a suit against the organization. In other instances, a third party can demand a ransom failure to which to damage the system or release stolen data.

Historical Incidences of cyber attacks

There are some notable Occurrences in the past that shaped the need for cyber risk management.

- Robert Tappan Morris and the Morris Worm (1988)- Creator of the first computer worm transmitted through the Internet where 6000 computers were reportedly affected causing an estimated $10-$100 million dollars in repair bills.

- The Melissa virus (1999)- a very simple virus which ended up costing $80 million in damages

- Solar Sunrise (1998)- systematic cyber attack was launched in the US which seized control of over 500 government and private computer systems.

-December 2015: A carefully designed cyber attack caused a power outage in Ukraine. 3-6h of black-out impacting 80.000 homes

-Feb 2016: Hackers stole $81M from Bangladesh national bank

-2015: Hackers stole $12M from Ecuador's Bancodel Austro

How and Why do hackers go scot free?

Cyber criminals have continued to enjoy some immunity for a long time due to several reasons:

- Attribution problem: it is almost impossible to gather conclusive evidence connecting a given individual to a cyberattack.

- It is difficult to bring cybercriminals to court, due to delays in international police cooperation procedures that are not compatible with IT speed, since evidence may be automatically erased after a few days or weeks.

-Most of the time the hackers could be located outside the legal jurisdiction of the court and prosecutors seeking the conviction. The prosecutors lack the legal powers to proceed with the suit. There are cross-boundary, reciprocal legal rules with many cyber allies, but many more countries don't and won't participate

-Having differences in interpretation of what is Lawful/Legal and unlawful/illegal for instance, if porn is illegal in a particular locality but is accessed on a computer that is located outside that locality, is it illegal? Is it prosecutable? Some local court systems say yes, but many more say no. For that reason, most smaller entities leave it up to the federal legal system to define and prosecute computer crime.

- The vast majority of internet crimes are never reported. Most people have no idea of where and how to report internet crime, and if they do, rarely does anything come of it. Because most internet crimes are not reported, accurate statistics and evidence are hard to come by -- even though they're needed to help in a successful prosecution.

-Gathering Legal evidence is a toll order as someone needs to address the following questions beforehand;

How can one confirm the log file hasn't been tampered with?
Who had the ability to access the log file?
Is the time and date stamp accurate? How does one know?

How can one ascertain that the computer system accurately detected the originating IP address -- can’t IP addresses be faked?
Was the log file originally written to write-once, read-only media?
What has been the chain-of-custody of that log file since it was first created until now?
What experience does the computer team have with obtaining legal evidence?

- Governments may even hire hackers for intelligence purposes, in exchange for protection against prosecutions for cybercrime.

Burden of Cyber Risk

The cost of cyber risks can be quantitative in the sense that they can be measured in monetary terms as listed below:
-Fines and Penalties
-Legal fees incurred in defense of law suits
-Reduced productivity as a result of poor sales
-Overheads which remain constant despite low production like salaries, bills, taxes.
-Revamped advertisements in an effort to salvage the company’s image
-Penalties imposed by the government due to lack of compliance.

There are however some costs which can be difficult to quantify in monetary terms and can be termed as qualitative in nature:
-Loss of intellectual property
-Tarnished brand image
-Weakened market share/position
-Effect on a customer/third party who fails to meet their deadlines as a result of the organization’s system interruption and is fined

Organizations globally are under extreme pressure from both the shareholders and other stakeholders to deliver on their mandate despite the threat of cyber risk. Firms have to maintain shareholders value, achieve new performance peaks, nurture employees to become topmost performers, satisfy customers needs, keep making new products and services as well as invest in communities.

How then can an organization meet all the above expectations?

The ultimate solution to this is in embracing Cyber Security best practices.

Unfortunately, the very essential strides that a company embraces to drive its agenda happen to be the ones that actually generate cyber risk threats.

It is worth noting that cyber risk cannot be totally exterminated, it can only be properly managed to ensure the smooth running of operations. The management needs to evaluate the following queries as they strive to embrace cyber security.

-To what extent can the company tolerate/retain any identified risk?

-How much is the organization willing to spend in terms of finances and personnel to manage the risk?

-In the unfortunate event a loss happens, would it be disastrous?

In terms of harm to employees, customers, suppliers, visitors, the public, brand image?

-Can the organization manage without technology and for how long?

The firm needs to make appropriate investments in security, vigilance and flexibility in order to ensure successful strategic growth and performance. This can only be effectively achieved if a company has a clear understanding of the threats facing the firm and their impact in the worst case scenarios.

Positioning an Organization in managing Cyber Risks

In modern business times, the success of any enterprise boils down to its ability to make informed decisions on cyber risk management. The business that is better positioned continues to enjoy continued growth whereas the firms that fail to embrace effective methods suffers dire consequences.

The various sources of cyber risks pose diverse levels of impact and this calls for prioritizing resources to manage and help mitigate likely outcomes. The areas to focus on are threefold:

-Organization internal organs: These are critical systems that contain the most sensitive data on all applications that help run all operations on the entire organization. Information on intellectual property, employees data, customers and suppliers information.

-Extended Information system: This could include supply chain management (SCM) applications, partner portals and systems extended to third parties.

-External systems like web pages and servers, systems accessible through the internet by the public.

The business needs to harness both tangible and intangible assets, human and financial and ensure compliance with policies and adherence to the legal and regulatory framework.

Whose responsibility is cyber risk management?

Management of cyber risk refers to the policies that counter vulnerabilities in information systems, programs and networks to ensure there is cyber security.

Since cyber risk is an area that touches more on information technology, it is assumed that the buck stops with the IT department. It is however the responsibility of every stakeholder in the business to ensure cyber security.

"It is everyone's responsibility to ensure cyber security within an organization"

Social networks and unlimited connectivity have seen to it that employees' work and social lives are no longer separate but have now been interweaved. Because of this, cyber security now rests with every employee to ensure their work and social data is safe.

Ways to guarantee cyber security

In today's world of immense cybersecurity risks, it is really important for enterprises to be pre-equipped with the security tools and privacy enhancements that are needed to safeguard their most valuable asset -data.

Outlined are ways to ensure cyber security:

-Educating employees on cyber security best practices.

-Regularly backing up the most important information like critical emails and shared data.

-Restricting user access. Employees are only required to access data they need.

-Securing networks by ensuring operating systems firewall is enabled. If employees work form remote access areas/ home, their home systems should also be protected by firewall.

-It's important to be cautious of clicking on any pictures on the internet, addresses, hyperlinks, pop-ups, ads and graphics. Some of them could be viruses and on clicking, the machine gets attacked.

-Running of anti-virus scans frequently and installing software updates regularly e.g once a month.

-It is very important to let anti-virus scans run to completion and allowing the system to reboot periodically.

-Limiting followers and access to social media. Employees need to beware of liking, following unfamiliar pages, or allowing different applications to access ones profile owing to the fact that not many internet users have proper cyber hygiene on cleaning them up when no longer required.

-Mobile users should password protect their devises, encrypt data and install security Apps.

-Being wary of public Wi-Fi by not selecting remember the Wi-Fi network. I addition, using the latest web browsers because they have improved security for fake browsers.

-Enabling privacy and security settings which are normally disabled on computers.

-Ensuring card readers are using modern EMV-chip technology which makes transactions safer

by creating unique transaction reference codes that cannot be used again.

-Limiting sensitive personal data on social media by only giving the basic information required to sign up accounts.

-Employing a password manager to help track the age of each password which ideally should be updated every nine months to one year. The password manager also assists in generating complex passwords for all accounts.

-Limiting social logins (single sign ons) where someone signs up for new accounts by using ones Google+ or Facebook.

-Desisting from providing one's passwords or personal information to unsolicited callers.

-Subscribing to identity protection

-Signing up for real-time alerts form the banks and credit card companies. This helps one track any unauthorized transactions in real-time.

-Routinely checking the credit card statements to determine if all purchases have been authorized by the owner.

-Using biometrics appropriately.

-Knowing one's digital footprint which refers to data that exists in cyber space as a result of actions and communications that one performs with others online.

-employing pinpoint to find the right technology partner of one's business.

-Using strong passwords and changing them periodically for instance every 3 months. A strong password should contain alphabets, numerical as well as special characters/symbols like @#!/.

-Performing daily full system scans.

-Creating a periodic system back-up schedule to ensure one's data is retrievable should an attack happen to ones machine.

-Regularly updating one's computer system to repair any bugs and abnormalities with the system.

-Installing anti-spyware and anti-malware software which specifically targets spyware and malware threats.

-Implementing the right technology that allows one to monitor third parties in real-time.

The above mentioned methodologies are internal policies and processes undertaken by an organization to safeguard its information system from cyber threats. By clearly identifying threats, a firm needs to understand what could happen should the threat materialize, proceed to quantify in monetary terms the cost of salvaging the effects of cyber sabotage. Ultimately, the organization needs to embrace effective cyber risk management practices and policies.

In addition to the above mentioned methods of enhancing cyber security, the firm needs to be properly positioned in terms of implementing cyber security controls to enable achievement of the targeted cyber security standards.

We now briefly list ways of implementing cyber security controls which will in turn guarantee cyber security which is the main objective of the organization.

- Having the ability to discover, identify and monitor all devices connected to the network. These may be all authorized and unauthorized devices like laptops, tablets and printers, sensors, IP cameras, heart monitors, infusion pumps. It's important to monitor the exact location of the various devices, their access restrictions, ability to detect abnormal behavior.

-Regular penetration tests within the company to gauge the organization's preparedness in countering attacks.

-Assessing data recovery ability.

-Ensuring secure configurations for network like installing firewalls

-Limitation and Control of Network Ports, Protocols, and Services

-Installing malware defenses

-Taking a detailed inventory of all authorized and unauthorized software connected to the network.

-Maintenance, Monitoring, and Analysis of Audit Logs.

-Ensuring limited number of users with access to privileged and highly confidential information.

-Continuous trainings to all users on ways to enhance cyber security.

-Ensuring emails and web browser protections.

The main objective of this coursework is to explore a cyber risk management method which is transfer of the risk through insurance which will be expounded on in detail in the following pages.

Cyber Risk Insurance

Businesses are different in terms of operations and so are the products/services on cyber insurance. Although there is no standard rule for underwriting these policies, the coverage offered normally cover two main areas;

-First Party Coverage- protects against losses suffered by the insured

-Third Party Coverage- protects against losses suffered by third parties.

Let's start by analyzing what is covered under first party cover.

- **Theft and Fraud**: This covers theft of data and extortion of the insured's funds. Unintentional distribution of the stolen data and trade secrets.
- **Investigation Costs**: A forensics investigation is necessary to determine the cause of loss of data, how to repair damage and how to prevent the same type of breach from occurring in the future. Investigations may involve the services of a third-party security firm, as well as coordination with law enforcement and the FBI.
- **Business losses:** A cyber insurance policy may include similar items that are covered by an errors & omissions policy (errors due to negligence and other reasons), as well as monetary losses experienced by network downtime.
- **Network and Business Interruption**. Covers the costs of business lost and additional expense due to an interruption of the insured's computer systems. Some cyber policies require that the interruption be caused by an intentional cyber attack and some do not. There could also be a requirement on time excess and cover is also subject to a set indemnity period.
- **Extortion**. Covers the costs of "ransom" if a third party demands payment to refrain from publicly disclosing or causing damage to the insured's confidential electronic data and intellectual property.
- **Lawsuits:** This covers legal expenses associated with legal settlements and regulatory fines.
- **Cost of Data Recovery:** This covers the costs of restoring lost data, diagnosing and repairing the cause of the loss.
- **Privacy Breach Notification:** Cover is provided for data breach notification to clients and other affected parties.
- **Repair of tainted company brand reputation:** costs associated with advertisements aimed at restoring back stained image.

We now look at the coverage offered to third party liability coverage.

- **Transmission of viruses coverage: C**over for liabilities arising from damage occasioned to third parties due to malicious virus transmission.

- **Notification costs:** Cover is provided to include costs of informing clients/third parties about data breach incidents. The cover here may limit the number of people to be notified and the means/modes of notifying them.
- **Governmental action**: Cover may be provided for any costs to be paid to the government for breaches of data, failure to adhere to regulatory measures and negligence-failure to exercise due diligence and protect the employees, clients.
- **Privacy liability cover:** This cover takes care of any liabilities arising from data breaches on employees, clients and suppliers private and sensitive information. The insured owes all these stakeholders a duty of care in ensuring their private data is well safeguarded.
- **Crisis Management:** Cover to strive to buy back the publics' confidence and trust after the fallout and try to mend ways. This extends to cover call centre charges

There are some important elements to take into consideration while signing up for a policy.

- **Choice of Counsel:** Insurers sometimes require the insured to only choose defense firms from their select panel of law firms to represent them in a legal suit. This is due to the substantial costs likely to be associated with a significant data breach case.

-**Trigger of a law suit:** Some policies will only respond if there is a demand letter or a suit levelled against the insured. This therefore means any defense that has not materialized into a suit is not covered.

-**Trigger of loss or a claim:** Some policies come into play if an actual loss or claim is made against the insured, event that triggers coverage is considered as well as the timing of the claim which will determine if the policy will respond or not.

-**Retroactive date cover**: Insurers normally limit their coverage to losses occurring after the retroactive date indicated on the policy which usually starts at inception of cover though an insured can negotiate for a date prior to inception at an additional premium.

-**Acts and Omissions of third parties:** If the insured relies on a system provided by a hired third party to store sensitive customers data, they (insured) need to have a cover that expressly extends coverage for data breaches occasioned by the third party system. Otherwise most of the policies will exclude breaches by such a system.

- **Unencrypted devices**: Coverage for losses emanating from machines whose data is unencrypted is normally excluded. It is therefore important to determine if cover is extended to cover such machines or not.

-**Policy Territory**: Majority of cyber policies limit their territorial scope to unites states of America. Coverage beyond the territory may only be granted at an additional premium. It is therefore important to understand the scope of the territory being covered.

-**Physical Location of breach**: Some policies only limit the location of breach to the insured premises only. This means virus attacks to laptops at home, while travelling, at the airport is not covered. Also theft of flash discs or external disks while one is travelling is not covered.

-**Acts or Omissions**: Some policies normally limit coverage for;

1. The insured's failure to take reasonable steps to design, maintain and upgrade its security

2.) Defects in security of which the insured was aware prior to the inception of cover.

3. Certain malfunctions of security software.

-**Acts of War or Terrorism**: In some policies this is an exclusion but can be bought back to ensure liabilities arising from acts of hostile/foreign nation is covered.

There are some extensions that can be offered in addition to cyber risk the standard cover.;

-Publication of credit card information

-Extortion (Ransom)

-Electronic Theft for Instance Internet banking

- Multimedia Liability

-Monitoring

-Intellectual Property Infringement.

Cyber Crime risk standard exclusions

There are standard exclusions which are excluded in a standard crime liability cover. However, some of them can be bought back by way of paying some extra premium.

-Prior and/or pending claims

-Improvement Costs-Bettering the risk than it was previously

-Business Interruption that is not caused as a result of cyber related incidences

-Bodily injury and property damage

-Violation of patent rights

-Unlawfully collected data

-Unauthorized trading

-Contractual liability

-Employees mistakes or criminal acts.

What's the Role of Insurance in the Cyber Domain?

-Improve the understanding of cyber risks (and a data base pertaining to them) overcoming inhibitions to disclose/share). Identify trends

-Employ its risk underwriting potential to establish benchmarks for good cybersecurity practices.

-Incentivize compliance with these standards.

-Underwrite cyber risk beyond physical damages and loss of business due to service disruption to cover to IP and even reputational damages

- Help identify aggregation risks.

- Harmonize behavior across nations and corporations (which no nationlregulation or legislation can do)

Areas of Interest to Insurers before providing cover

Insurers would like to advance coverage to an organization that has a cyber risk profile. This is where the enterprise has analyzed its susceptibility to cyber attacks and has employed best practices to ensure any would be attacks are dealt with soonest possible and claims are minimized.

An organization that embraces employee trainings and awareness about cyber security is also likely to receive favorable terms and wider coverage.

An enterprise that conducts threat intelligence oftenly is better placed to be prepared to counter any possible cyber attacks.

An Insurer may require an audit of the company's processes, procedures and mode of governance. This gives an insurer some insight into cyber risk tolerance of the firm.

Underwriting Challenges

Underwriters need:

-An understanding of the Insured's business model in order to conceptualize the risk;

-Exposure data [of various types] in order to price the risk;

-Risk control information to assess the risk

-Sense of the loss context to undertake the risk.

It is important, particularly in the case of claims made on the eve of policy renewal, to precisely define which factual events trigger coverage. Current policy language is inconsistent, and most policies are on a claims-made basis, which increases the potential for mixed triggers (a claim could be filed when a loss is discovered, or when a system is compromised).

The industry needs to be able to more accurately value loss. Forensic investigation commissioned by or on behalf of the insured is meant to establish the cause and extent of a breach, but it does not address the financial impact on the insured.

The way clauses are applied also needs to be examined. A policy with primary coverage that has a war and terrorism exclusion with a buyback clause for cyberterrorism could include excess coverage that does not. This can result in disputes over payment of claims. Further, the utility of such clauses is limited due to difficulties with attribution.

There is discontinuity between primary and excess markets. There is no loss adjuster appointed on behalf of the market, which results in the primary insurer acting in its own best interest to the detriment of the underwriters of the excess coverage.

Cyber insurance is bundled into existing products. In order for the risk to be better understood and quantified, specific cyber products are required in place of silent coverage within existing products. Silent coverage is a significant problem because the potential cost could be considerable unless a policy has sub limits and clear wording. Simply adding clear cyber exclusions to policies, which might be difficult in this market to do that anyway, is inadequate in itself, since our customers require coverage.

Pricing models should be based on a close examination of the risk that needs to be underwritten and validation of the risk to the extent possible using available data. Conceptually, there is no barrier to developing pricing models around first-party dependencies and values, but most of the market is still using professional liability rates. If the industry does not have robust pricing models in place now, it will not be ready when it needs to transfer the pricing of cyber exposures into the automobile market, for example.

Conclusion

The insurance industry is going through a difficult transition in which we do not have adequate profitability to invest in new risk. We should be optimistic. The industry has tackled many new risks in the past, so we can tackle at least some of these new risks, as well as the traditional risks that are regenerating. Our challenges are to obtain the right resources, adapt our culture, and offer reliable solutions that, at the same time, appeal to our customers and are viable for us over the long term.

A potential insured seeking coverage approaches an insurer and the it is a requirement to have a cyber risk proposal form completed to allow further negotiations. What is contained in a cyber proposal from?

Cyber Risk Questionnaire/Proposal Form

Outlined below are the common queries contained in a cyber questionnaire.

1. Insureds General Information

-Name of proposer/organization
-Physical Location-country, city, street, building. Addresses-telephone number, emails.
-Date of business establishment
-Details regarding any mergers/acquisitions and any such planned exercises in the near future.
-Any involvements in joint Ventures-Details on how all processes, procedures and policies have been integrated into the parent/main group system.
-An summary of the business activities carried out at the firm on a daily basis.
-The number of employees including casuals and contractors/sub-contractors involved.
-Details of revenue generated in the last financial year, current and projected gross income in the following year.

2. Data Information

-Details on the number of data records stored in the system-basic personal employees data, sensitive information on employees health, firm's trade secrets, payment card information, financial as well as third parties like clients, suppliers, debtors, the government and adjacent community.

-The proposer is required to disclose if employee/client data is shared with third parties, whether it is anonymized prior to sharing, for what purposes is the shared data used for.

-What due diligence the proposer takes to ensure the recipient of the shared data has cyber secure environment.

3. Network Exposure

-The amounts generated via online platforms in terms of sales, commissions, donations, Fees.
-The level of fluctuations in the online revenues and by what percentage. At what point the revenues are at the highest.

-In case of any network disruption, the amount that would be at stake at any given time.
-What steps the Insured takes to prevent big time outages like having a back-up system
-The additional costs that would be incurred to minimize the impact of disruption.
-Any disaster recovery plans and processes.

4. Third party Exposure (outsourced service provider-OSP)

-Information on Data services outsourced to third parties.
- What due diligence is undertaken before engaging with a new outsourced service provider
-How data is stored-whether in private cloud or in shared servers.
-If data breach occurs, whose responsibility is to do notifications and who bears the costs?
- If an OSP system or cloud service is unavailable, what is the likely impact on the insured
-The business recovery measures in place following cloud failure.

5. Data Security

-Monitoring of sensitive data on the network
-Whether the confidential data stored on the servers/data bases is encrypted when stored and during transmission
-Whether critical data is backed-up at least weekly.
-Whether the insured maintains back-up tapes/cassettes/disks
- Access to highly sensitive data is only given to very few senior staff upon authorization.
-Whether there is a Chief Privacy Officer or who runs that function.
-Details on compliance with various bodies like Health Information Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach Bliley Act (1999), Fair and Accurate Credit Transactions Act (FACTA), Payment Card Industry Data Security Standards
-Description of data retention and destruction policy.
-Whether the insured maintains user revocation procedures on user accounts following employee termination.

6. Network Security
-Whether the insured utilizes firewalls, Anti-Virus or Anti-Malware
- Network access controls for remote access
-Whether the insured enforces a ‘strong password policy’ requiring passwords of adequate complexity and length.
-Confirmation of carrying out server and application security configuration hardening
-Whether the organization maintains a Whitelist to prevent malicious software and other unapproved programs from running
-A description of the process of managing and installing patches on systems and applications
-Use of any unsupported operating systems or software

-Disablement of USD drives to employees
- Whether the organization has a Social Media presence

7. Security Policies and Procedures

-If the insured has a cyber-threat intelligence gathering function
- Is regular penetration testing carried out by a 3rd party? When last performed, any serious concerns raise on the last one carried out and what remedial steps have been taken to address such concerns
-Maintenance of any certified information security standards.
-Any regular security assessments carried out by a 3rd party? When last performed, any serious concerns raise on the last one carried out and what remedial steps have been taken to address such concerns
-Any continuous awareness training programme for employees regarding data privacy/security, including legal liability and social engineering issues
- performing of background verification checks for all candidates of employment, contractors and 3rd party users

8. Points of Sale (POS) and Merchants (Only for users of credit cards for Payments)

-Confirmation of being fully compliant with EMV card processing standards
-Whether the POS systems have anti-tampering features
-Confirmation that the POS devices regularly scanned for malware or skimming devices
-Requirement for formal approval to changes to the POS systems
-Information on whether POS network assessed by a 3rd party
-Any high level vulnerabilities on the POS system and how they have been addressed.
-Whether the POS system developed and maintained by a PA-DSS compliant vendor
-Description of how payment card data is captured and transferred to the credit card processor, including the encryption and/or tokenisation process
-Whether changes on individual files on the POS system create alerts in real-time
-If the POS systems have anti-tampering features

9. Incident Response and Claims History

-Any incidences in the last 5 years relating to;

-Unauthorized disclosure or transmission of any confidential information

-Negligent or unintentional act or failure to act by an employee or an employee of any third party service provider whilst operating, maintaining or upgrading the computer system.

-suspension or degradation of the computer system

- Your inability to access data due to such data being deleted, damaged, corrupted, altered or lost

-Any receipt of extortion demand or security threat

- Receipt of a claim in respect of any of the above

- Any formal or official action, investigation, inquiry or audit by a regulator arising out of the use, control, collection, storing, processing or suspected misuse of personal information

-Whether the insured has any incident response plan which includes a team with specified roles and responsibilities and if it has been tested in the last 12 months.
-If the Insured maintains incident log of all system security breaches and network failures

10. Limits of Liability Required

The limit of Liability requested will be determined by the level of exposure foreseen, the system controls in place and any history of loss incidents. It follows that a higher limit will see the insured pay relatively higher premium due to the high risk being transferred to the insurer.

The Insured then consents to the declaration by appending their signature, company stamp and date. The proposal form is then forwarded to the insurer to be analyzed and revert with terms and/or their advises.

The Insurer can offer coverage for a cybercrime policy based on 2 primary policy forms;

-Claims Occurring basis

-Claims made basis

- A cyber crime policy on a claims occurring basis meets claims that occur during the policy period regardless of when the claim is made. It covers claims that have occurred during a period of cover even if the claim is made after the cover has been lapsed or cancelled.
- A policy on Claims Made basis meets claims that are made and reported during the policy period for work undertaken after the retroactive date shown on the policy. The Retroactive Date is usually the date at which cover was first incepted. At each renewal the same Retroactive Date is carried forward. This cover will not provide cover for any claims after a policy has been lapsed or cancelled as there is no policy in force when the claim is made. It is therefore important to consider purchasing a ‘run off’ cover. This will

cover claims after the lapsing or cancelling arising from work occurring prior to lapsing or cancelling.

A different Perspective on Cyber Insurance

Cyber insurance is not unique as a product. It covers losses that exhibit similar patterns to certain others covered by standard insurance. Indemnification for data loss notification or event management is not that different from the product recall coverage that might exist as an extension in some product liability policies. Cyber extortion is not dissimilar to kidnap and ransom in terms of indemnification process and service provided to the insured. Computer fraud could be covered by a crime or fraud policy.

The indemnification principle for Business process disruption due to an IT network interruption is similar to the one for Business Interruption following a property damage. Data or computer restoration costs are not unlike replacement costs of any asset covered by a property policy. Privacy or Security liability claims are substantially similar to an E&O claim.

First, cyber risks are strongly linked to intangible assets, which represent a growing portion of every company's assets. For this reason, the insurance market must focus more on how to value and insure data and intellectual property, and how to quantify reputation damage and determine whether or not it can be insured.

Second, non-physical losses are commonly covered, but we must ensure that the industry has the expertise to indemnify business interruption due to a cyberattack without material damage. We must also face conflicting interests that may exist between criminal investigation and preservation of evidence on one hand and prompt business recovery on the other hand.

Third, we must be ready to cope with the very dynamic threat landscape in which risks are not only increasing, but also changing in nature. This includes increasingly pervasive technology. With connected objects, cyber risk is now entering the physical world, and attacks may result in material damage, bodily injury, and circumstances that are currently covered by existing policies. We need to examine whether standard policies are able to respond to this risk.

Finally, systemic risk is a key issue and risk propagation is an intrinsic feature of cyber risks developing in an interconnected world. We must explore how to manage the accumulation of risk due to common vulnerabilities or cascading effects.

We have so far addressed cyber risk insurance and our next move will focus on cyber risk management.

Cyber Risk Management

Definition: Risk Management is the process of identification, analysis, assessment, control, avoidance and minimization of cyber risk exposure within an organization.

The enterprise needs to assess the likelihood and potential impact of a cyber risk exposure and then determine the best approach to deal with the risks. Given that cyber risk cannot be entirely eliminated, risk management should come into play in tackling the effects of uncertainty on organizational objectives in a way that makes the most effective and efficient use of limited resources.

First and foremost, the organization needs to be aligned with its main goals and objectives which sets the right foundation for effective risk management process. The company needs to adopt a cyber risk strategy which addresses six main key areas.

- Identification and assessment of the firm’s tangible and intangible core assets.
- Develop a cyber risk appetite i.e. Determine what magnitude of risk the firm is willing to accept and retain.
- Assessing the profile of cyber attackers or in a nutshell find out the likelihood of cybercrime damage that would be suffered should it happen.
- Based on point number 3 above, the firm needs to assess their preparedness and defense strategies in mitigating cyber threats.
- Measurement and Quantification-This is estimating the severity of possible cyber threats in monetary terms.
- Having clearly analyzed, assessed and quantified the effects of a cyber threat, it is important for an enterprise to consider the best response methods in managing cyber risks e.g. risk retention, transfer (Insurance), loss mitigation measures (educating staff).

Considerations for Effective Risk Management Process

- Speedy response: Response to counter attacks should be timely in terms of early detection, speedy mitigation measures taken and recovery plans. This calls for thorough preparedness.
- Elasticity: An organization should endeavor to continue operating during and after the disruptive periods. It should withstand tough market times and deliver on its mandate amid the operational stress and disruption.
- Continuous Trainings: The Organization needs to embrace a culture of regular trainings to enhance cyber security throughout the company.
- Communication Processes: An enterprise needs to have clear lines of detecting threats, communicating the same to the relevant personnel who in turn take the necessary

action and if the matter seems out of hand, to escalate the same to higher authorities. All through, all staff should be kept in the know how on what's happening.

- An Organization should have its priorities right owing to the fact that there are limited resources in terms of staff and funds. Prioritizing enables the company allocate adequate resources towards managing cyber threats.
- Investing on Intelligence: The company requires to engage in continuous intelligence tests to enable timely detection of any cyber threats both internally and externally. Some cyber penetration tests should be carried out frequently to establish the level of preparedness in countering any possible threats.
- Maintaining cyber hygiene: Implementing basic cyber hygiene practices is a good starting point for cyber risk management. It aids in timely detection of threats, effective reduction of any impact should there be any attack.

How can an organization maintain Cyber Hygiene?

The Center for Internet Security (CIS) defines cyber hygiene as a means to appropriately protect and maintain IT systems and devices and implement cyber security best practices.

There are various ways that can enhance cyber hygiene as outlined below;

-Making use of complex passwords that contain a minimum of 8 characters ranging from numerical, alphabetical, symbols and special characters.

-Limiting the number of users with access privileges to highly sensitive and confidential data.

-Blocking installation of new software by users without prior approval from the head of IT department.

-Continuous trainings to all staff on ways of maintaining cyber security like always logging off their machines after work, locking the machines when not in use for some time, ways to identify potential phishing efforts.

-The company should maintain a record of all hardware and software on the organization's network.

- Identify vulnerable applications that aren't in use and disable them.

-Making sure data is always backed up and having several copies of the same data to enable one access the original copy should there be any threat to the system.

-Adoption of Industry's accepted configurations standards like NIST and CIS benchmark.

-Patching all applications immediately and regularly to minimize incidences of attacks.

-Ensuring the system is always upgraded to newer versions as the aging ones have already been well mastered by potential hackers.

Five steps of cyber Breach Response Escalation Plan

- Pre-Breach Response Planning

- Identify Internal Response Team & Incident Lead Person

- Establish Analysis and Communication Protocol

- Complete Data Breach Response Plan

- Evaluate Vendor and Customer Notification Requirements

- Remediation and Recovery Vendors

- Stress Test Response Plan

- Fraud Prevention

- Incident Analysis

- Contact the Team

- Identify Information (Payment Card compromised)

- Breach Containment

- Harm Determination Forensic Analysis

-Legal Analysis

- Security Breach Incident Analysis

- Incident Disclosure

- Analyze Requirements

- Consider Alternative Notice Methods

- Notify in compliance with laws

- Consider third-party vendors for notification

- Stagger Notification

- Public Reporting

- Cyber Insurance Carrier Notification

- Loss Mitigation

- Credit Monitoring

-Fraud Monitoring

-Documentation and discoveries manifest

-Customer Service

-Human Resources

▪ Communication and Remediation

-External Solutions

-Customer protection and notification letter

-Customer hotline number establishment

-Breach website

-Senior management updates

-Human Resource updates

-Cyber Insurer briefing

-Directors and Officers Liability Insurer briefing (If Material)

-Limit Communication

Question 1:

How Your company managed to protect itself against different types of cyber risks.

An Insurance company is an organization that handles massive amounts of data ranging from the prospects/proposers' personal information, Insureds personal details, employees' data, suppliers, debtors and creditors information as well as third parties details.

Such a huge organization cannot run the daily operations without the assistance of an information system to aid in data processing, storage and transfer of information. This therefore means such a company can be a major target for cyber attack owing to the vast amount of data contained in the system.

There are measures taken by our organization to shield the enterprise from cyber attacks which will be highlighted below:

- Continuous training of staff on various ways to minimize cyber risk attacks. Below is an excerpt of a circular done by the head of IT to all staff mid 2017.

"CYBER SECURITY ALERT

Dear team,

In an effort to further enhance our company's cyber defenses, we want to highlight a common cyber-attack that everyone should be aware of – phishing. "Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal – getting you to share sensitive information such as login credentials, credit card information, or bank account details.
Although we maintain controls to help protect our networks and computers from cyber threats, we rely on you to be our first line of defense. We've outlined a few different types of phishing attacks to watch out for:

- *Phishing: In this type of attack, hackers impersonate a real company to obtain your login credentials. You may receive an e-mail asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.*
- *Spear Phishing: Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name and phone number and refer to APA in the e-mail to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.*

- *Whaling: Whaling is a popular ploy aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, they look like normal emails from a high-level official of the company, typically the GCEO, CEOs or CFOs, and ask you for sensitive information (including usernames and passwords).*
- *Shared Document Phishing: You may receive an e-mail that appears to come from file sharing sites like Dropbox or Google Drive alerting you that a document has been shared with you. The link provided in these e-mails will take you to a fake login page that mimics the real login page and will steal your account credentials.*

What actions to take….

To avoid these phishing schemes, please observe the following email best practices:

- *Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.*
- *Do not provide sensitive personal information (like usernames and passwords) over email.*
- *Watch for email senders that use suspicious or misleading domain names. There is currently a lot of spam (unsolicited emails) going round. Do not open these emails if you cannot verify authenticity of the sender.*
- *Inspect uniform resource locators (URLs) carefully to make sure they're legitimate and not imposter sites.*
- *Do not try to open any shared document that you're not expecting to receive.*
- *If you can't tell if an email is legitimate or not, please do not open the email and contact IT support for assistance.*
- *Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.*

Thanks again for helping to keep our network, and our people, safe from these cyber threats.
Please let us know if you have any questions."

- In addition to point 1 above, the Organization has invested heavily in back-up servers that guarantee availability of data should there be an attack and data is lost.
- There is a fully fledged IT department that is mandated with the responsibility of ensuring any cyber threats are addressed in a timely manner.

- The company has ensured installation of anti-virus, anti-malware and anti-spyware on all machines of staff.
- There is a requirement to change all users' passwords every three months and no password can be used more than once. The passwords have to meet the company's set standard of complexity in terms of length-minimum of eight characters, inclusion of special characters e.g. @#!.
- There is also limited access to highly confidential and privileged information on trade secrets, company assets, employees' health records.
- All emails sent using the company address have a disclaimer which states as under-" *This e-mail, including attachments, is intended for the person(s) or company named and may contain confidential and/or legally privileged information. Unauthorized disclosure, copying or use of this information may be unlawful and is prohibited. If you are not the intended recipient, please delete this message and notify the sender. Please note that any opinions, express or implied, presented are solely those of the author and do not necessarily represent those of APA Apollo. Every proposer whilst seeking new insurance or renewing an existing Policy must disclose any information which might influence APA in deciding whether or not to accept a risk. The proposer is solely responsible for any information provided. Failure to make appropriate disclosures may render the insurance voidable from inception and enable APA to repudiate liability on claims presented. Unless advised otherwise, it is understood by APA that the proposer or insured is acting on their own behalf and has appropriate authority to do so. All incoming and outgoing e-mail messages are stored in our Mail Archives. If you do not wish the retention of potentially private e-mails by us, we strongly advise you not to use the APA Apollo e-mail accounts for any private, non-business related communications."*
- Once an employee attempts to log in to a machine and they use incorrect password, one is allowed to attempt a minimum of 3 times after which one gets locked out and can only be reset again by IT personnel.
- Staff are only allowed to access necessary data on their line of duty that is stored on shared networks. For instance, there could be Underwriting folder, Marketing, Claims Medical insurance and agriculture folders. If a staff works in finance department, they are restricted from accessing all the above mentioned folders as they do not need the information contained therein.
- Once an email is sent to any user within the organization that could have some virus, any attachments on such an email do not open and one is referred to IT for assistance. This means there is timely and effective detection of cyber viruses.
- There are restrictions on what sites the company's browser can log onto. If a user attempts to search an unauthorized site, the browser will give a warning and one cannot proceed.
- Staff are also restricted in terms of using flash disks, CD players and connecting any external systems to their machines without consent from head of IT.

- All staff machines have the same wallpaper and no staff is allowed to install features of their choice. There is a standard wallpaper and background colour.
- Machines automatically log off/lock after 10 minutes if not in use and when one resumes, it is a requirement to log in again using one's password.
- The IT staff routinely take an inventory of all machine on the network at any one point. No machine is allowed to log onto the network without being approved by the head of IT.
- When an employee leaves/ceases work, their password, log-in credentials are disabled/deactivated and no one can use them to log onto a machine.
- The organization has embraced use of newer application versions like windows and word 2016.

There are some challenges to overcome as the organization strives to enhance cyber security.

- Need to raise cyber expertise in the Organization.
- Improvement of Risk Management process and quality of information
- Collection of data & Building of risk models
- Manage risk aggregation and exposure to Cyber Cat

Once the above noted challenge are addressed, the company will be better placed to enjoy some benefits as outlined under.

- Offer tangible solutions to clients.
- Leverage digitalization to enhance company's operations
- Become a player among the best Insurers in the market
- Improve knowledge and market share on cyber risk.

Question 2:
New products of Cyber Insurance for specific industries (Supply chain, Banks, Petrochemicals, Hotels, etc)

The uniqueness in industries in terms of operations calls for customized cyber policies to cater for the needs of each segment. There is no standardized approach on cyber insurance which means that the product offered to like a bank might differ with one offered to a restaurant, hospital or a Legal firm.

We shall briefly address some few select industries by highlighting the ideal coverage suitable for such an industry.

- **Banks:** On 10th April 2018, there was a statement issued jointly by the Federal Reserve, FDIC, OCC, NCUA and CFPB through their affiliation in the Federal Financial Institutions Examination Council (FFIEC) alerting banks of risk management issues regarding cyber insurance coverage.

The regulators did not require banks to take up cyber insurance but it did propose consideration of uptake of the cover to take care of some losses stemming from customer identity theft, fraud and even extortion. These losses would result in income decreases, lawsuits, regulatory fines and reputation damage. Each bank is to involve multiple stakeholders within its organization for example, legal, risk management, IT and financial staff to review the bank’s existing control environment and related cyber risks.

Banks normally take up Bankers Blanket Bond policy to cover majority of its risk exposure under one umbrella and at times there can be an extension on BBB to cover cyber risks or it can be taken as a stand-alone product.

The management of a bank should consider the following factors before settling on any cyber insurance product:

-Identify loopholes for cyber threats and sample some coverage that can address such gaps.

-Get to fully understand what will be the triggers of losses covered, the sub-limits, exclusions on the policy and the premium chargeable.

-Before effecting cover, it is important to find out if the Insurer is well capitalized and of good claims paying ability history.

-It is important that the management of the bank understands that taking up an insurance policy does not mean that they are absolved of their mandate to continuously enhance cyber security within the organization.

- **Hotels:** The hospitality industry is highly dependent on electronic processes and computer networks in the daily operations to aid in marketing their facilities, online bookings and payments, they also gather and maintain private information about their clients. The hospitality industry also engages vendors, contractors and third party service providers.

A typical dining area in a restaurant

Some of the cyber risks associated with this industry emanate from;

-Payments by use of credit cards
- Disclosure of Personal identification information while booking hotel rooms
-Points of sale machines
-Online payments for hotel bookings
-Employee Information on personal details
-Third Party Information-Suppliers, vendors and contractors.
The ideal cyber insurance coverage for hotel industry can be divided into 2 policies:

- First Party Coverage: As earlier on explained in this paper, first party coverage extends to cater for the following risks:
  -Loss of income due to failure of network security
  -Network business interruption
  -Data restoration costs
  -Response management costs associated with public relation consultants to assist in restoring the tainted brand image, Forensic costs, call Centre/notification costs
  -Cyber Extortion
- Third Party Coverage: This covers the following;
  -Liability arising out of defamation and infringement of intellectual property rights.
  -Fines and Penalties arising out of privacy breach regulatory proceedings

- Failure of computer network security to guard against threats such as hackers, viruses, worms, Trojan horses and denial of service attacks whether or not resulting from the provision of professional services.
- Wrongful disclosure of Personally Identifiable Information, Protected Health Information or confidential corporate information in the client's care, custody or control via a computer network or off-line.

- **Petrochemicals:**

The oil, gas and petroleum industry has not been spared from cyber threats/attacks. It is important to look into 2 areas while addressing industrial cyber risk.

- Information Technology (IT): relating to computing technology such as networking, hardware, software and internet. This combines all computer abilities to collect, process and present information for decision making purposes across a business organization.
- Operational Technology (OT): Industrial Control System (ICS) which support physical value creation in manufacturing processes largely in the form of automation. The ICS comprises all necessary hardware and software to control and monitor process equipment.

The ICS includes the following;

-Supervisory Control and Data Acquisitions Systems (SCADA) – used throughout the oil, gas and petrochemical industry to display information from controlling systems to the plant operator through a human machine interface (HMI), in some industries such as pipeline operation the SCADA will also be used for its control functionality

-Distributed Control Systems (DCS) – again used throughout the oil, gas and petrochemical industry for facility control, alarm and in some cases emergency shutdown purposes (i.e. Integrated Control & Safety Systems (ICSS)). DCS systems are optimized to handle high volumes of complex process logic

- Programmable Logic Controllers (PLC) - used for equipment specific control and safety functions such as emergency shutdown (ESD), either standalone (local) or communicating to DCS or SCADA. For a PLC being used for a critical ESD function the safety instrumented systems (SIS) is optimized for speed and reliability.

Cyber attackers can target the following areas;

-Equipment Sabotage: A hacker could implant false data showing that there had been a breakdown in the equipment in a remote facility, leading the victim company to waste time and financial resources investigating.

- Plant Destruction: A cybercriminal could engineer an oil explosion by increasing the maximum filling limit of an oil tank.

- Oil Market Fraud: Malware can fake data about the amount of oil a company has in stock to make the quantity appear much bigger than it actually is. Once the victim company runs out of oil, it won't be able to deliver to its customers. Failure to satisfy its obligations could wreak havoc and lead to changes in oil prices, as well as huge losses to the company.

Here are some of the risks a company may face in the case of a successful attack:

-Undetected spills

-Utilities interruption

-Production circle shutdown

-Inappropriate product quality

-Equipment damage

-Safety measures violation resulting in injuries and even death

-Plant shutdown

There is need to establish good general IT security procedures for the ICS, these should include the following:

-Backing up control system software

-Controlling access to engineering workstations

-Controlling access to the ICS

-Blocking USB and / or other access points to the ICS

- Management of mobile devices

The firm should also invest heavily in a cyber risk insurance policy to cater for unforeseen costs like business losses, investigation costs, network and business interruption costs, extortion of funds, privacy breach notification and other coverage as earlier mentioned in this paper.

- **Supply chain:** It is important to understand the context of a business supply chain i.e. what the environment the business operates in dictate about cyber risks- product's use, what it is connected to, and who the users are.

  - How the product will be used; The focus is on what type of data will be managed in the system. Essentially, the company needs to determine the consequence of the data being compromised or leaked outside of the system.
  - How the system is connected to the rest of the world; A system that is connected to the public internet will need more reliable security, since it would be easy to find and attack. On the other hand, a system that is isolated from any other network would have a much lower risk of attack or data breach, since the attacker would need to be in physical proximity of the system.
  - Who the system users are; Are the users internal employees who are trained on security procedures, or is the system accessed by a public user base which may not consider risky security behaviors? Simple security procedures, such as keeping passwords secret and maintaining current anti-virus software, cannot be counted on if the management does not directly control the users' environment.

  It is also important to dig into the developers' coding practices, whether the developer has ensured enough safeguards are in place to prevent the discovery, or exploitation of vulnerabilities in their apps or software.

Premeditated & Political Challenges to Promoting Interstate Cyber Norms

-Broad, generic, cultural divides in attitudes toward norms
-Complexity of issues, and diversity of domestic stakeholders
-Conflicting visions over utility, indispensability, and cost/risk associated with cyber weapons and warfare
-Fundamental divergence over what constitutes cyber warfare (versus information security): linkages & priorities
-Number and diversity of pertinent players internationally

-Complexity of issues associated with handling non state actors (proxies, private sector entities, NGOs, criminals)

Offensive action by States can contribute to cyber insecurity. Code is left behind after a cyberattack, and the victims can learn from this and retaliate. However, when confronted with a choice between traditional and cyber warfare, the latter may be a more attractive option for States. Such acts could serve a legitimate national security purpose when used – selectively and responsibly – not only for intelligence, but also for offensively targeting equipment in wartime situations. In the current climate, governments must not launch attacks lightly. Several factors could encourage major players to show restraint, including ethical and legal concerns, their own vulnerability to retaliation, the difficulty in accurately identifying foes (misattribution), fear of blowback (systemic effects), and fear of compromising their own capabilities or sources.

While conflicts and crime are increasingly being channeled into cyberspace, States and institutions are weakening. States are under pressure, challenged, and often unable to regulate within their own territories. If States do successfully regulate internally, without international agreement, their rules may be ignored, sidestepped, or interpreted in widely different ways. There has also been a significant increase in companies offering offensive services to States or corporate clients: those who have significant technological, operational and financial capabilities are developing their skills and offering. These actors are operating in countries where rules are lax and engaging in offensive cyber operations is tolerated.
Perhaps the most serious issues we are facing going forward are the general undermining of confidence and trust, and the manipulation of integrity of data, which is rare, but increasingly worrisome.

On the Private Sector Front….

For technology companies like Microsoft, governments are both major customers and Advanced Persistent Threats (APT). Companies must maintain a relationship of trust with governments through transparency and neutrality. It is essential that governments understand that the role of technology providers is not to take sides in the geopolitical debate. Their sole interest in this context should be cyber defense and security.
Governments need to be smarter about procuring information technology, and they need to spend more money to update it. It is also imperative that companies invest in cybersecurity, although certain factors will remain beyond their control, such as users failing to update or upgrade software. The cloud offers a viable alternative to maintaining and securing in-house IT infrastructure. It can offer significant advantages, such as stronger security models and redundancy.

What's the Role of the Government in enhancing Cyber Security?

Governments should be at the fore front in implementing programs to increase the cybersecurity of organizations and to assist in the aftermath of attacks. Governments are offering incentives to companies to beef up their security, or assisting them in doing so.

Governments have put in place mechanisms whereby certain organizations can call on outside Computer Emergency Response Teams (CERT) to assist with response or mitigation if they believe they have been attacked by a state.

It is of utmost importance for governments to develop and implement a Cybersecurity National Action Plan that spells out actionable plans to be undertaken by a well funded body to mitigate the effects of cyber risks.

It is the role of the government to come up with legislation on cyber security and enforce its adherence by all stakeholders within a country. Hefty fines and penalties should be levied organizations that fail to meet the minimum requirements.

The government can in addition to the above outlined responsibilities rollout a cyber awareness campaign, extend the campaign to learning institutions by implementing a subject to be examined in all learning institutions.

Every day, cybercriminals carry out large-scale economic surveillance to undermine the competitiveness of companies. These attackers, who come from a wide range of origins, infiltrate IT and communication networks to steal important or vital company information. They often start to lay the groundwork for their attacks with social engineering, which is manipulating or tricking people into revealing information or performing some action. They have access to people and a great deal of information that is freely available online, particularly through professional social networks like LinkedIn. On such sites they can obtain information on strategic projects, employee responsibilities, technologies used, and identify vulnerabilities they can exploit.

Sabotage

Acts of sabotage can constitute acts of war or terrorism, and this is the case in an international security context. However, it is easier to attack Critical National Infrastructure (CNI), such as mass transport, banking systems and power grids, than it is to attack military targets. An attack on CNI could have devastating effects. The consequences of the shutdown of a national power grid or water distribution system would be dire: beyond the economic impact, there would also be loss of life.

A business needs to invest heavily in business risk intelligence which covers the broader risks to the organization, ranging from insider threats to the physical security of executives and staff, or the risk of engaging with third-party vendors in the supply chain.

Finally, the Organization should adhere to the set guidelines on its cyber security strategy.