Credibility . Professionalism . AccountAbility

Cyber Security & Internal Audit – Is the Blame on Systems?

Agenda

- What is cyber security
- Pillars of cyber security
- Why is cyber security important
- Global risk outlook
- Cyber security attacks
- Myths vs Reality
- Role of Internal audit
- How do we protect ourselves?

What is cybersecurity

- The state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.
- Cyber security consists of technologies, processes and controls designed to protect systems, networks, programs, devices and data from cyber attacks.
- Effective cyber security reduces the risk of cyber attacks and protects against the unauthorised exploitation of systems, networks and technologies.

Pillars of Cyber Security

- Robust cyber security and information security involves implementing controls based on three pillars:
- People, processes and technology.
- This three-pronged approach helps organisations protect themselves from both organised and opportunistic attacks.

Pillars of Cyber Security

- **People-** Every employee needs to be aware of their role in preventing and reducing cyber threats, and staff dedicated to cyber security need to keep up to date with the latest cyber risks and solutions.
- **Processes:-** Documented processes should also clearly define roles and responsibilities, and specify the procedure to follow when, for example, reporting a suspicious email.
- **Technology-** technical controls are essential. From access controls to installing antivirus software, technology can be deployed to mitigate cyber risks.

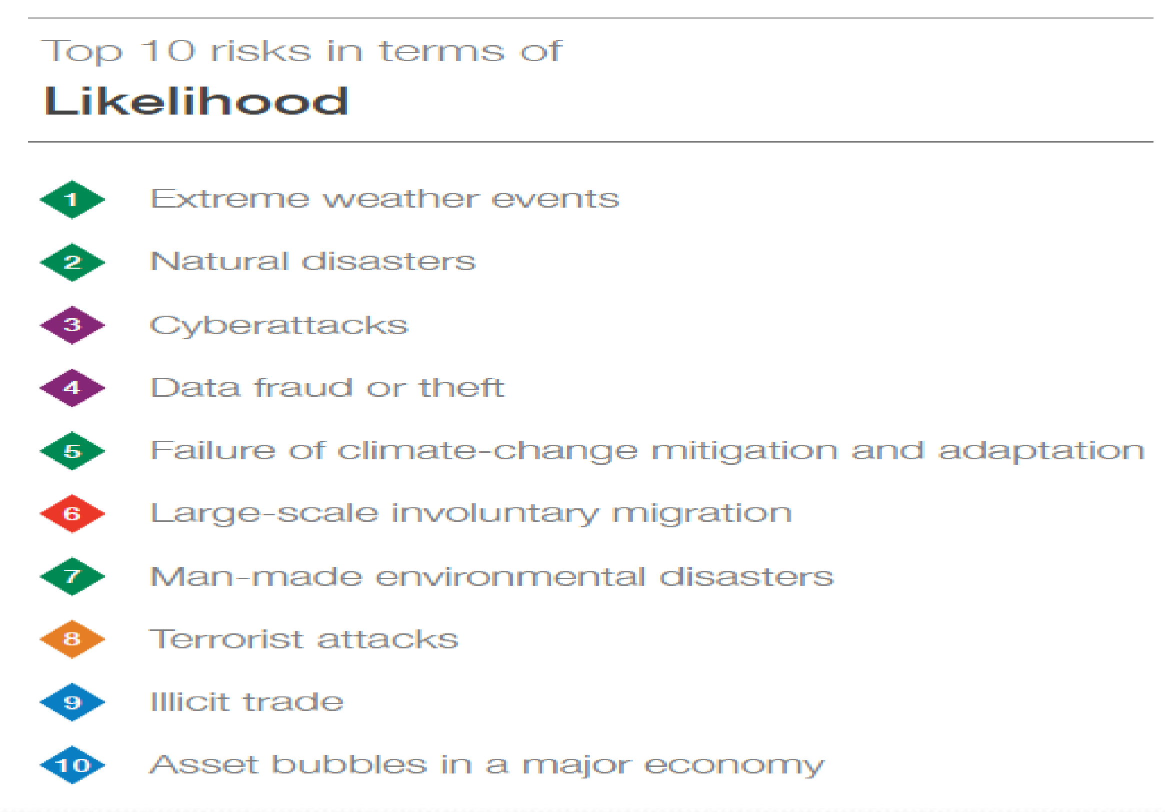
Why is cyber security important?

- **The costs of data breaches are soaring-** Emerging privacy laws can mean significant fines for organisations. (talk to British Airways, $240 million fine for data breach)
- **Cyber attacks are becoming increasingly sophisticated -**Cyber attacks continue to grow in sophistication, with attackers using an ever-expanding variety of tactics, including social engineering, malware and ransomware.

Why is cyber security important?

- **Cyber attacks are lucrative-** Usually, cyber attackers seek some type of benefit and will invest in various techniques, tools and technology to achieve their motives. Financial gain is a common motivation, but they may also be driven by political, ethical, intellectual or social incentives.
- **Cyber security is a critical, board-level issue -** New regulations and reporting requirements make cyber security risk oversight a challenge.
- The board will continue to seek assurances from management that their cyber risk strategies will reduce the risk of attacks and limit financial and operational impacts.

Global Risk outlook 2019

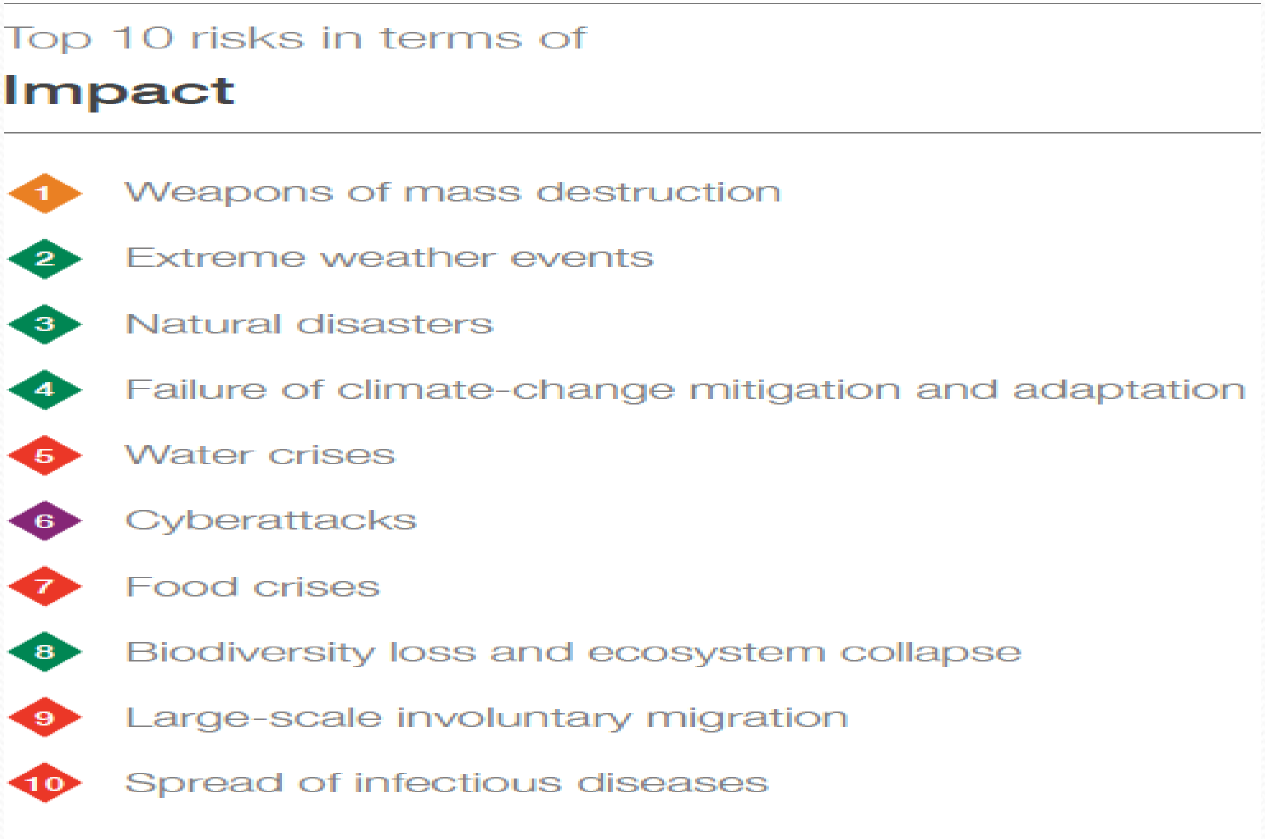


Top 10 risks in terms of

Likelihood

1. Extreme weather events
2. Natural disasters
3. Cyberattacks
4. Data fraud or theft
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Man-made environmental disasters
8. Terrorist attacks
9. Illicit trade
10. Asset bubbles in a major economy

Global Risk outlook



Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Extreme weather events
3. Natural disasters
4. Failure of climate-change mitigation and adaptation
5. Water crises
6. Cyberattacks
7. Food crises
8. Biodiversity loss and ecosystem collapse
9. Large-scale involuntary migration
10. Spread of infectious diseases

What are the Cyber attacks and cyber security threats

- Below are a few common cyber attacks and threats.
- **Phishing-** This is an old but still popular tactic. It is a social engineering attack that tries to trick people into divulging sensitive or confidential information. Not always easy to distinguish from genuine messages, these scams can inflict enormous damage on organisations
- **Social engineering-**Social engineering comes in more forms than just phishing, but is always used to deceive and manipulate victims in order to obtain information or gain access to their computer. This is achieved by tricking users into clicking malicious links or by physically gaining access to a computer through deception.
- **DDoS (distributed denial-of-service) attack-** A DDoS attack attempts to disrupt normal web traffic and take a site offline by flooding a system, server or network with more requests than it can handle.

What are the Cyber attacks and cyber security threats

- **Ransomware -** One of the fastest-growing forms of cyber attack, ransomware is a type of malware that demands payment after encrypting the victim’s files, making them inaccessible.
- **MITM (man-in-the-middle) attack -** An MITM attack occurs when a hacker inserts themselves between the communications of a client (device) and a server. MITM attacks often happen when a user logs on to an insecure public Wi-Fi network. Attackers are able to insert themselves between a visitor’s device and the network. The user will then unknowingly pass information through the attacker.
- **Virus -** A virus is a piece of malicious code that is loaded onto a computer without the user’s knowledge. It can replicate itself and spread to other computers by attaching itself to another computer file.

Biggest Cyber security crises of 2019 so far

- **Customs and Border Protection Contractor Perceptics** **-** In May, a surveillance contractor for US Customs and Border Protection suffered a breach, and hackers stole photos of travelers and license plates related to about 100,000 people.
- **Ransomware** **-** Ransomware attacks are truly nothing new at this point, but 2019 is looking like a banner year for them. Criminal groups continue to target businesses, health care providers, and, most visibly, local governments with these brash hacks, in which malware is used to encrypt a system's data and then demand a ransom to decrypt it.

Biggest Cyber security crises of 2019 so far

- **American Medical Collection Agency breach - **One of the most concerning corporate data breaches so far this year is that of the American Medical Collection Agency, a massive health-care-related debt collector. The incident was first publicly reported at the beginning of June after the medical testing firm LabCorp said that 7.7 million of its customers had data exposed because of AMCA, and Quest Diagnostics said it had had records from 12 million patients exposed.
- **First American-** Not all data security incidents are breaches. Sometimes data is improperly stored and publicly accessible—it may not have been stolen, but it was still exposed. And First American, the massive real estate and title insurance firm, offers a crucial cautionary tale of how dangerous data exposures can be. Discovered in May by security journalist Brian Krebs, the incident exposed 885 million sensitive customer financial records going back to 2003.

Recent Cyber attacks in Kenya

- **“Communications Authority sounds alarm over cyber-attacks in Kenya” (standard newspaper April 2019) -**The October-December 2018/19 statistics released by the authority shows an increase in the number of cyber threats targeted at Kenya’s cyber space with over 10.2 million cyber events detected during the quarter as compared to 3.8 million in the previous quarter.
- The cyber threat events detected varied from Denial-of-Service (DOS) attacks, which hampered the availability of computer services, and online abuse, which included online fraud, hate speech, incitement to violence and fake news.
- “Kenya Lost 21.2 bn trough cyber attacks in 2017” – Capital News

Recent Cyber attacks in Kenya

- KRA -4Billion - In 2017 KRA reported that cybercriminal made away with about KES 4Billion.
- NBK –29 Million- In a statement, the bank said the breach saw the hackers make away with KES 29 Million but did not detail how the breach had occurred adding that they were “confident” they would recover most of the money.
- CBK –In 2013,theCBK suffered a major breach when its website was taken over by a cyber-based group known as the Gaza Hacker
- Mobile fraudsters - These use mobile phones to perform identity theft and other phones of social engineering attacks

Mistake/Myths Vs Reality

Mistake/Myths	Reality
We have to achieve 100% security.	100 percent security is neither feasible nor the appropriate goal.
When we invest in best-in-class technical tools, we are safe.	Effective cyber security is less dependent on technology than you think.
Our weapons have to be better than those of our attackers.	The security policy should primarily be determined by your goals, not those of your attackers.

Mistake Vs Reality

Mistake/Myths	Reality
Cyber security compliance is all about effective monitoring.	The ability to learn is just as important as the ability to monitor.
We need to recruit the best professionals to defend ourselves against cybercrime	Cyber security is not a department, but an attitude
We only engage the most reputable firms who are capable of managing information security.	The responsibility of information security cannot be outsourced.

Role of Internal Audit

Internal audit has a critical role in helping organizations in the ongoing battle of managing cyber threats, both by providing an independent assessment of existing and needed controls, and helping the audit committee and board understand and address the diverse risks of the digital world.

Role of internal audit

❖The threat from cyberattacks is significant and continuously evolving.

❖Many audit committees and boards have set an expectation for internal audit to understand and assess the organization’s capabilities in managing the associated risks.

❖Experience shows that an effective first step for internal audit is to conduct a cyber risk assessment and distill the findings into a concise summary for the audit committee and board which will then drive a risk-based, multiyear cybersecurity internal audit plan.

How do we protect ourselves?

- Exploring an organization’s cyber risks begins with three key questions:
- Who might attack? Are the perpetrators criminals, competitors, third party vendors, disgruntled insiders, agenda-driven hackers, or someone else?
- What are they after, and what business risks need to be mitigated? Do they want money or intellectual property? Is their goal to disrupt the business or ruin our reputation? Could health and safety risks be created?
- What tactics might they use? Will they go phishing, test system vulnerabilities, use stolen credentials, or enter networks through a compromised third party?

Three pronged approach

- Secure- Most organizations have established controls such as perimeter defenses, identity management, and data protection to guard against known and emerging threats. Risk-focused programs prioritize controls in areas that align with top business risks.
- Vigilant-Threat intelligence, security monitoring, and behavioral and risk analyses are used to detect malicious or unauthorized activity such as application configuration changes or unusual data movement, and help the organization respond to the shifting threat landscape.
- Resilient- Incident response protocols, forensics, and business continuity and disaster recovery plans are put into action to recover as quickly as possible and reduce impact.

Pillar #1-Secure

Attributes	Key considerations
Cybersecurity risk and compliance management	• Compliance monitoring • Risk and compliance assessment
Secure development life cycle	• Secure build and testing • Secure coding guidelines • Security design/architecture • Policy and standards management
Third party management	• Evaluation and selection • Security assessment • Ongoing monitoring
Information and asset management	• Information and asset classification • Physical media handling • Physical an environmental security controls • Information records management
Identify and access management	• User access management and governance • Privileged user access management • User recertification

Pillar #2 -Vigilance

Attributes	Key considerations
Threat and vulnerability management	• Incident response and forensics • Application security testing • Threat modelling and intelligence • Security event monitoring and logging • Vulnerability and penetration testing
Data management and protection	• Data classification and inventory • Breach notification and management • Data loss prevention • Data security strategy • Data encryption • Records and mobile device management
Risk analytics	• Information gathering and analysis around: –User, account, entity - Events/incidents - Fraud and anti-money laundering - Operational loss

Pillar #3 Resilient

CPAK

Credibility . Professionalism . AccountAbility

Crisis management and resiliency	• Recover strategy, plans and procedures • Testing and exercising • Business impact analysis • Business continuity planning • Disaster recovery planning
Security operations	• Change management • Configuration management • Network defense • Security operations management • Security architecture
Security awareness and training	• Security training • Security awareness • Third-party responsibilities

Questions?

ICPAK

Credibility . Professionalism . AccountAbility