Journal of Positive School Psychology
2023, Vol. 7, Issue 1
Pp 163-171

Analysis of the cyber security challenges and solutions

Shabana Kausar
PhD Scholar at Dada Bhoye Institute of Higher Education Karachi and Lecturer at Institute of Law University of Sindh Jamshoro Sindh Pakistan
Ali Raza Leghari
PhD scholar at SZABUL Karachi and Assistant Professor at Institute of Law University of Sindh Jamshoro Sindh Pakistan
Erum Iftikhar
Lecturer at School of Law, University of Karachi Sindh Pakistan

Abstract
During 2020 world experienced a big change in trends due to pandemic. World introduced use of technology in every level even in education use of technology increased and due to this excessive use of technology introduced concept of smart cities. By the increased use of internet cyber-attacks also increased and during Lock down strategy for covid-19, cyber hackers' activities increased and ransom is also introduced. Hackers attack on business and most prominent websites. DDos attacks are could be targeted, hackers' attacks on different systems and for the purpose to getting remote control hackers introduced malware in target and covert them in botnet and encrypt the useful data and demand ransom to decode it. Pakistan is also under the threat of such cyber-attacks and working on cyber security is need of time.

Keywords: Cyber, Security, Malware Attacks, Cyber Law, Vulnerability, System, Smart City.

Article History:
Received: 9th Feb. 2023
Accepted: 10th Mar. 2023
Published: 02nd Apr. 2023

1. Introduction:

With growing technology day by day threat of cyber-attacks on national international and personal level is also increasing. Pakistani citizens are also big users of interne technology and simple innocent peoples are soft target of cyber attackers. There are many types of cyber-attacks. Some basic rules may apply on cyber-attacks as under:

Where there is vulnerability in system there is cyber-attacks.
Every system which is connected with internet and other computers is under vulnerable
Where there is trust there exist exploitation
With each new innovation new threats of cyber-attack increased
Whenever doubtful things come in the way always vulnerability.

World leading websites are under the attacks of cyber hackers. There is need of making cyber security laws to prevent such attacks. During covid-19 cyber security is no more a technical issue at all and it now becomes a serious issue. Internationally companies are facing losses that are doing e-business. This problem is growing on daily bases. Firms or companies which are now also leading companies now a days ensure that take on board those who know about cyber security and technically aware about risk in the e-business context, their impact and how the leaders address them. There are eleven common cyber attacks

Cyber-attacks are malicious activities carried out by individuals or groups with the intent of compromising, damaging, or gaining unauthorized access to computer systems, networks, or data. There are numerous types of cyber-attacks, each with its own distinct methods and objectives. Some common types of cyber-attacks include:

1. Malware Attacks: Malware, short for malicious software, is designed to infiltrate systems and cause harm. Common types of malware include viruses, worms, Trojans, ransomware, spyware, and adware.
2. Phishing: Phishing attacks involve tricking users into revealing sensitive information, such as login

credentials or financial data, through deceptive emails, websites, or messages.

3. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: These attacks overwhelm a targeted organizations network or its system by too much emails and unnecessary traffic or excessive requests, causing it to become unavailable to legitimate users.
4. Man-in-the-Middle (MitM) Attacks: This attack is made by the attacker intercepts and possibly alters communications between two parties, making them believe they are directly communicating with each other.
5. SQL Injection: Attackers insert malicious SQL code into input fields of web applications, exploiting vulnerabilities to access or manipulate databases.
6. Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, potentially compromising their browsers and stealing sensitive information.
7. Zero-Day Exploits: These attacks take advantage of unknown vulnerabilities in software or hardware before the developers can release a patch.
8. Advanced Persistent Threats (APTs): APTs are long-term, targeted attacks in which adversaries gain unauthorized access to a system and remain undetected while extracting sensitive information.
9. Ransomware Attacks: Malicious software encrypts a victim's data, and the attacker demands a ransom for the decryption key.
10. Social Engineering: This technique involves manipulating individuals into divulging confidential information, often exploiting psychological and emotional factors.
11. IoT-Based Attacks: Cybercriminals exploit vulnerabilities in Internet of Things (IoT) devices to gain unauthorized access to networks or launch other attacks.
12. Eavesdropping/Sniffing: Attackers intercept and monitor network traffic to obtain sensitive information.
13. Brute Force Attacks: In these attacks, automated tools try all possible combinations of passwords until the correct one is found, gaining unauthorized access to accounts.
14. Credential Stuffing: Attackers use lists of stolen login credentials from one website to attempt unauthorized access to accounts on other websites where users have reused passwords.
15. Drive-By Downloads: Users unintentionally download malware when visiting infected websites or clicking on malicious links.
16. Watering Hole Attacks: Attackers compromise a website frequently visited by their target audience to distribute malware to the site's visitors.
17. Keylogging: Malicious software records keystrokes on a victim's device, capturing sensitive information like passwords and credit card details.
18. Fileless Attacks: These attacks operate in memory, leaving no trace on the victim's hard drive, making them harder to detect.

2. The concept of smart city and its protection

Smart city term is use for such city which uses technology to provide services and solve problems of citizens. A smart city has to do efforts to improve transportation services and accessibility, improve social services, promote sustainability, and give its citizens a voice. Though the term “smart cities” is new, the idea.

By developing smart cities and growth of technology leads to the conditions where expense of cyber security is increasing for all medium to large scale working companies in all over the world over the past five years. According to a new study by the RAND Corporation, companies are spending more and more on cyber security tools. Thus, global cyber security costs close to $70 billion a year and grow annually at a level of 10-15%. Activist groups, or “hacktivists”: Are not usually out to steal the money. They’re out to promote their religion, politics or cause; to impact reputations or to impact clients.

As mentioned earlier, a smart city is a city that employs digital technologies and data-driven solutions to enhance the quality of life for its residents, optimize city operations, and promote sustainable development. The core idea of a smart city is to leverage information and communication technologies (ICT) and the Internet of Things (IoT) to improve various aspects of urban life, including transportation, energy efficiency, public safety, healthcare, education, and more. The integration of these technologies aims to provide better services, increase efficiency, and create a more connected and sustainable urban environment.

Now, let's explore how to protect citizens from cyber-attacks in a smart city:

1. Cybersecurity Framework: Establish a comprehensive cybersecurity framework that encompasses all layers of the smart city infrastructure, including devices, networks, data centers, and cloud services. This framework should include security policies, guidelines, and standards for all stakeholders.
2. Secure IoT Devices: Given the prevalence of IoT devices in a smart city, it's essential to ensure their security. Manufacturers and developers should follow best practices for secure device design, including strong authentication mechanisms, encryption, and regular software updates to address vulnerabilities.
3. Network Security: Implement robust network security measures, such as firewalls, intrusion detection systems, and encryption protocols, to protect data as it travels between devices and data centers.
4. Data Protection: Data is a valuable asset in a smart city. Apply encryption and access controls to safeguard sensitive data. Limit data collection to what is necessary and ensure proper anonymization or pseudonymization when storing or processing personal data.
5. User Education: Educate citizens about potential cyber threats and promote responsible digital behavior. Citizens should be aware of phishing attempts, social engineering, and the importance of strong passwords.
6. Multi-Factor Authentication (MFA): Require multi-factor authentication for accessing critical services and data. This additional layer of security helps prevent unauthorized access, even if passwords are compromised.
7. Incident Response Plan: Develop a well-defined incident response plan to handle cyber-attacks effectively. This plan should outline roles and responsibilities, coordination with relevant authorities, and recovery procedures.
8. Collaborative Approach: Encourage collaboration between city authorities, private organizations, and cybersecurity experts to share threat intelligence and best practices. A joint effort can strengthen the overall cybersecurity posture of the smart city.
9. Regular Audits and Penetration Testing: Conduct periodic security audits and penetration testing to identify vulnerabilities and address them before malicious actors can exploit them.
10. Continuous Monitoring: Implement real-time monitoring of smart city systems to detect unusual activities or signs of a cyber-attack promptly.

By adopting these cybersecurity measures, a smart city can better protect its citizens from cyber threats and ensure a safer and more resilient urban environment. It is essential to proactively address cybersecurity concerns to maintain the trust of residents and stakeholders in the smart city's infrastructure and services.

During lockdown and pandemic peoples in all over the world are facing business losses and so also they are losing their loved ones. On other hand Hackers become very active and they caused very heavy loss to famous Brands. A NETSCAPE Arbor report suggested there were 7.5 million DDoS attacks in 2017, so while many target IT service providers, they are still more prevalent than many people realize. One of the most worrying aspects of DDoS attacks for businesses is that without even being targeted, the business can be affected just by using the same server, service provider, or even network infrastructure.

3. Research methodology:

This research is completed by analyzing available literature and Qualitative method is applied and results are described by descriptive method. Purpose of this study is identifying core cyber security Risk and all possible solutions by legislation and Digital Forensic.

Graphical presentation:

It could be presented in symbols and relations as:

All humans could be the seta, the Humans (H), the Servers (S), and the Information (I) which are elements of the Internet and growth (G) of Things. Essentially, we have:

H= Hn, S=Sn2, I=¼, G= increasing Hn

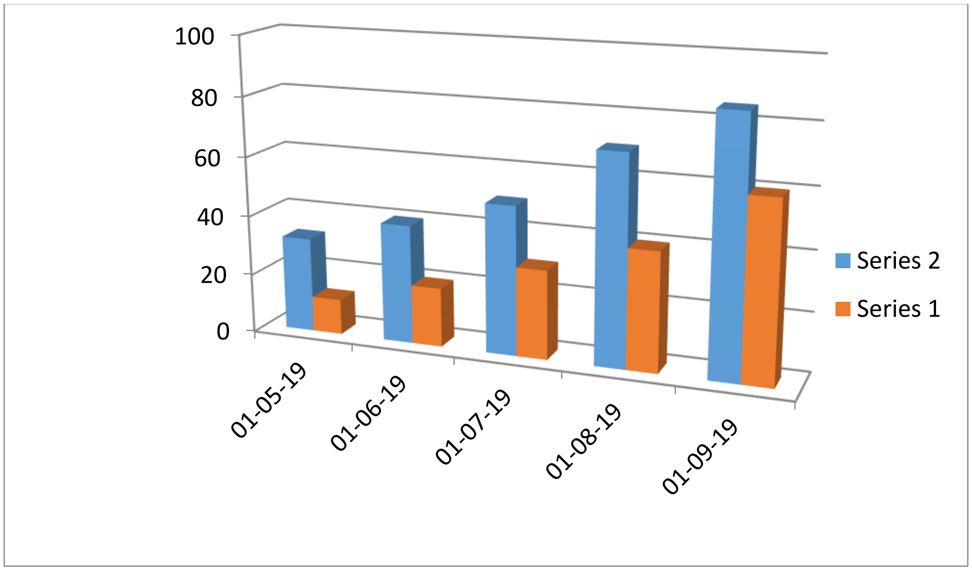
where: S < H I since there are less servers than persons and much less persons than thing in the emerging Internet of Things. The traditional Security and Privacy concerns are focused on protecting the vertices of the following within graphs:

GH by fire walls, anti-virus and so on.

Here in graph things are ignored as only focus is on humans by attackers. The outward relation graphs representing interactions or exchange of data between persons-servers and Humans-Information are represented below:

series 1 denotes Humans (internet users)
series 2 denotes Information

The interconnected information is growing in numbers, GHI and GSI are becoming extremely important and almost intractable. Our focus in the near future will be on protecting the servers of these graphs to create secure and privately acceptable Smart Cities.



Results and discussion:

Here the important discussion is the outcome or result of these issues with connection of online date transportation and real time activities. Smart transportation, public and private, has access to a website of interrelated data including monetary, GPS, vehicle state (within various parameters), weather and traffic updates.

4. Cyber security problems:

As technology continues to advance, so do the cyber threats and challenges that the world faces. Cybersecurity problems are constantly evolving and adapting to exploit new vulnerabilities and attack surfaces. Some of the key cybersecurity problems in the world include:

1. Sophisticated Cyber Attacks: Cybercriminals and state-sponsored actors are continually developing more advanced and sophisticated attack techniques, making it challenging for organizations to defend against them.
2. Ransomware Epidemic: Ransomware attacks have become widespread, causing significant disruptions and financial losses to individuals, businesses, and governments. Cybercriminals scramble and codify data to demand a ransom for its release.
3. Internet of Things (IoT) Vulnerabilities: The increasing adoption of IoT devices has created a larger attack surface, and many of these devices have weak security measures, making them susceptible to exploitation.

4. Supply Chain Attacks: Cybercriminals are targeting third-party vendors and suppliers to compromise the supply chain and gain access to larger organizations' networks and sensitive data.
5. Insider Threats: Employees or individuals with access to an organization's systems and data can pose a significant security risk if they misuse their privileges or become malicious insiders.
6. Nation-State Cyber Espionage and Warfare: Nation-states are engaged in cyber espionage and cyber warfare, targeting critical infrastructure, government entities, and private organizations.
7. Lack of Cybersecurity Awareness: Many individuals and businesses still lack sufficient awareness and knowledge about cybersecurity best practices, making them more susceptible to social engineering and phishing attacks.
8. Shortage of Skilled Cybersecurity Professionals: There is a global shortage of qualified cybersecurity professionals, making it challenging for organizations to build and maintain strong security teams.
9. Legacy Systems and Software: Aging and unsupported software and systems can pose significant security risks as they may have unpatched vulnerabilities and lack modern security features.
10. Mobile Device Vulnerabilities: With the widespread use of mobile devices, attackers are targeting smartphones and tablets with various malware and phishing attacks.
11. Cloud Security Concerns: As organizations increasingly adopt cloud services, ensuring the security of cloud-based data and applications becomes a critical challenge.
12. Data Breaches and Privacy Concerns: High-profile data breaches have exposed sensitive information of millions of individuals, raising concerns about data privacy and protection.
13. Lack of Cybersecurity Regulations and Standards: The absence of comprehensive cybersecurity regulations and standards in many regions leaves organizations without clear guidelines for protecting their systems and data.
14. Emerging Technologies Security: The rapid adoption of emerging technologies like artificial intelligence, blockchain, and quantum computing presents new security challenges that require careful consideration.
15. Cybersecurity for Critical Infrastructure: Critical infrastructure sectors, such as energy, transportation, and healthcare, are increasingly at risk of cyber-attacks that could have severe real-world consequences.

Addressing these cybersecurity problems requires a collaborative effort among governments, businesses, organizations, and individuals. It involves implementing robust cybersecurity practices, investing in cybersecurity education and training, promoting information sharing, and staying vigilant in the face of ever-evolving threats.

Use of Digital Forensic to solve Cyber Security Problems:

Digital forensics is a branch of forensic science that focuses on the recovery, investigation, and analysis of digital evidence from electronic devices and digital media. It involves the application of scientific and investigative techniques to collect, preserve, examine, and interpret data that can be used as evidence in legal proceedings. Digital forensics is commonly used in cyber security to investigate and solve various cyber security issues, such as data breaches, cyber-attacks, hacking incidents, and other cybercrimes.

Here's how digital forensics is used in solving cyber security issues:

1. Incident Response: When a cyber security incident occurs, digital forensics is employed to quickly identify the nature and extent of the attack. Investigators analyze logs, network traffic, and system data to understand how the attack occurred, what data was affected, and the techniques used by the attackers.
2. Evidence Collection: Digital forensic specialists collect and preserve evidence from compromised systems or networks. This process ensures that the evidence is admissible in a court of law, if necessary, and maintains the chain of custody to avoid contamination or tampering.
3. Malware Analysis: Digital forensics involves analyzing malicious software, or malware, to understand its behavior, capabilities, and how it spreads. This analysis helps in developing effective countermeasures and protection against similar threats in the future.
4. Attribution and Tracking: Cyber-attacks can originate from various sources. Digital forensics techniques can be used to trace the origin of the attack and potentially identify the attackers or their location. This information is crucial for law enforcement and intelligence agencies to pursue legal action.
5. Data Recovery: In cases where data has been deleted or encrypted by attackers, digital forensics can attempt to recover lost or encrypted data. This process is essential for restoring operations and understanding the full impact of the breach.
6. Log Analysis: Examining system and network logs is a vital part of digital forensics. Logs can provide

valuable information about the sequence of events leading up to and during an attack, helping investigators reconstruct the incident timeline.

7. Forensic Analysis of Devices: Digital forensics involves the examination of various devices, including computers, smartphones, tablets, and other digital media, to extract evidence relevant to the investigation.
8. Expert Witness Testimony: Digital forensics experts may be called upon to testify in court regarding their findings and the integrity of the evidence collected during an investigation.

Overall, digital forensics plays a crucial role in cyber security, enabling organizations to understand cyber incidents, identify vulnerabilities, and take appropriate measures to enhance their security posture and prevent future attacks. It helps in both reactive responses to incidents and proactive measures to prevent potential threats.

This course rhetorical course ought to be introduced in our universities because it is appropriate for each new comers to laptop security and laptop forensics and practitioners World Health Organization would like to any their skills. It covers sensible skills for network security, penetration testing and digital forensics, in addition because the theory and scientific basis that underpins everyday observe. It conjointly ensures that students have a basic understanding of the legal and regulative needs and therefore the standards bearing on laptop security.

5. International Level:

International cyber warfare refers to the use of cyber capabilities by one nation-state against another for military, political, economic, or strategic purposes. It involves the deliberate exploitation of computer systems, networks, and digital infrastructure to disrupt, damage, or gain advantage in conflicts between nations. These cyber operations can range from espionage and information gathering to disruptive attacks and even attempts to disable critical infrastructure

International cyber warfare refers to the use of computer-based attacks, espionage, and other cyber operations by one country or state-sponsored entities to target and disrupt the information systems, infrastructure, and networks of another nation. These cyberattacks can be conducted for various reasons, including intelligence gathering, economic espionage, political manipulation, and sabotage.

A notable case study of international cyber warfare is the Stuxnet attack, which came to light in 2010. Stuxnet was a highly sophisticated and complex computer worm designed to target Iran's nuclear program, specifically its uranium enrichment centrifuges. It is widely believed to have been a joint effort between the United States and Israel.

Stuxnet was designed to exploit several zero-day vulnerabilities in Microsoft Windows operating systems and Siemens industrial control systems (specifically, Programmable Logic Controllers or PLCs) used in Iran's nuclear facilities. Once it infected a system, it would spread through USB drives and network connections, eventually reaching the target PLCs. The worm would then manipulate the centrifuges, causing them to spin at erratic speeds, leading to mechanical failures and damage, without raising suspicion.

The Stuxnet attack was groundbreaking because it demonstrated the capability of using cyber means to target and disrupt critical infrastructure, in this case, a nuclear facility. It highlighted the potential for state-sponsored cyber attacks to have real-world consequences beyond just stealing information or disrupting communication networks.

As an act of cyber warfare, Stuxnet raised ethical and legal questions about the use of such tactics, the potential for collateral damage, and the implications of using cyber weapons against other nations' critical infrastructure. It also sparked debates about the need for international norms and regulations to govern cyber warfare.

It is important to note that while the Stuxnet case study gained significant attention due to its high level of sophistication and impact, there have been numerous other instances of international cyber warfare or cyber-espionage conducted by various nation-states targeting each other's governmental, military, and commercial entities. Cyber warfare continues to evolve rapidly, making it a prominent challenge in the realm of international relations and security.

Certainly! Here are five notable cases of cyber-attacks:

1. WannaCry Ransomware Attack (2017): The WannaCry ransomware attack in May 2017 was one of the most widespread and damaging cyber-attacks in history. It targeted computers running Microsoft Windows by exploiting a vulnerability in the operating system. The ransomware encrypted files on infected machines and demanded a ransom payment in Bitcoin to unlock them. It affected hundreds of thousands of computers worldwide, including hospitals, government agencies, and businesses, causing significant disruption and financial losses.
2. NotPetya Cyber Attack (2017): The NotPetya cyber attack, also known as ExPetr or Petya, occurred in June 2017. Like WannaCry, it utilized an exploit called EternalBlue to spread across networks. However, NotPetya was more destructive as it was designed to permanently encrypt and destroy data on infected systems rather than just extort money through ransom payments. The attack caused widespread damage to businesses in Ukraine and worldwide, affecting various industries, including shipping, finance, and energy.
3. SolarWinds Cyberattack (2020): The SolarWinds cyberattack was a highly sophisticated supply chain attack that came to light in late 2020. Malicious actors compromised the software build system of SolarWinds, a prominent IT management software company, and inserted a backdoor into their Orion product updates. This backdoor allowed the attackers to gain access to the networks of SolarWinds customers, including numerous U.S. government agencies and major technology companies. The attack exposed sensitive data and raised concerns about the security of software supply chains.
4. Sony Pictures Hack (2014): In November 2014, a group calling themselves the "Guardians of Peace" conducted a cyber attack on Sony Pictures Entertainment. The attackers breached the company's network, stole large amounts of data, and leaked sensitive internal documents, employee emails, and unreleased films. The attack caused significant embarrassment for Sony Pictures, exposed confidential information, and led to the cancellation of the theatrical release of the movie "The Interview," which depicted a fictional plot to assassinate North Korean leader Kim Jong-un.
5. Ukrainian Power Grid Attack (2015 and 2016): In December 2015 and again in December 2016, cyber-attacks targeted Ukraine's power grid. The attackers used malware to gain access to control systems and remotely manipulate equipment, leading to widespread power outages. These attacks were among the first instances of cyber-attacks directly affecting critical infrastructure, demonstrating the potential for cyber warfare to impact essential services and national security.

These cases illustrate the diverse nature and potential consequences of cyber-attacks, ranging from large-scale ransomware campaigns and supply chain compromises to politically motivated hacking and attacks on critical infrastructure. They highlight the importance of cybersecurity measures and international cooperation to address the evolving threat landscape.

6. Conclusion:

Cyber space is developing day by day and use of internet is at its peak. World has witnessed too many incidents of cyber warfare and cyber security lapse including Pakistan. Still no solid steps have been taken in this regard. All business areas are presently affected by ICT in present days. Cyber security risk can damage economy and national security of any country easily. About all billionaires are connected to ICT by one or other way. Cyber threats are emerging to man kind and should be dealt on National level. Only paper work is done to build a strong cyber policy since 2003. Strong implementation of cyber laws and policy is need of time as cyber space become heaven for criminals and cyber terrorist to recruit, collect funds, mobilize and psychologically initiate warfare. Research revealed that Pakistan is surrounded by hidden enemies and vulnerable due to unsecure cyber space. The bell of cyber war is already rung and it is the prime duty of Pakistan to secure cyber-space as soon as possible and frame a legal policy.

7. Recommendations:

Controlling cybersecurity problems requires a comprehensive and proactive approach. Here are some key recommendations to improve cybersecurity and mitigate potential cyber threats:

Risk Assessment and Management: Conduct regular risk assessments to identify and understand potential vulnerabilities and threats. Develop a risk management strategy that prioritizes critical assets and focuses on addressing high-impact risks first.

Employee Training and Awareness: Educate employees about cybersecurity best practices, the importance of strong passwords, how to recognize phishing attempts, and the risks associated with social engineering. Well-informed employees are the first line of defense against cyber threats.

Regular Software Updates and Patch Management: Keep all software, operating systems, and applications up to date with the latest security patches. Many cyber attacks exploit known vulnerabilities that could have been prevented with timely updates.

Use of Multi-Factor Authentication (MFA): Implement MFA wherever possible, especially for privileged accounts and critical systems. MFA adds an extra layer of protection by requiring users to provide additional verification beyond just a password.

Firewalls and Network Segmentation: Deploy firewalls and use network segmentation to limit access to sensitive data and critical systems. This helps prevent lateral movement by attackers within the network.

Data Encryption: Encrypt sensitive data at rest and in transit to protect it from unauthorized access. Encryption ensures that even if data is compromised, it remains unintelligible to unauthorized parties.

Incident Response Plan: Develop and regularly update an incident response plan that outlines the steps to take in case of a cyber incident or data breach. Test the plan through simulated exercises to ensure its effectiveness.

Backup and Recovery: Regularly back up critical data and systems, and verify the integrity of backups. Having reliable backups is crucial in case of ransomware attacks or data loss incidents.

Vendor and Supply Chain Security: Assess the cybersecurity practices of third-party vendors and partners, especially those with access to sensitive data or systems. Ensure they meet appropriate security standards.

Continuous Monitoring and Intrusion Detection: Implement security monitoring and intrusion detection systems to detect and respond to suspicious activities in real-time.

Implement Access Controls: Restrict access to sensitive data and systems based on the principle of least privilege. Limit access to only those who require it to perform their duties.

Regular Security Audits and Penetration Testing: Conduct periodic security audits and penetration tests to identify weaknesses and address them before attackers can exploit them.

Security Awareness Training for Management: Ensure that management is aware of the cybersecurity risks and the importance of investing in robust cybersecurity measures. Adequate budget allocation for cybersecurity initiatives is crucial.

Collaborate and Share Information: Work with other organizations, government agencies, and cybersecurity experts to share threat intelligence and best practices. Collective efforts can strengthen the overall cybersecurity posture.

Compliance and Regulatory Standards: Comply with relevant cybersecurity regulations and standards that apply to your industry. Adhering to established frameworks can guide your cybersecurity efforts.

By following these recommendations and fostering a culture of cybersecurity vigilance, organizations can significantly reduce their exposure to cyber threats and better protect their assets and data. Cybersecurity is an ongoing process, and it requires continuous monitoring, adaptation, and improvement to stay ahead of evolving threats.

References

1. Anderson, R., & Moore, T. (2006). The Economics of Information Security. Science, 314(5799), 610-613.
2. Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company.
3. National Institute of Standards and Technology (NIST). (2020). NIST Special Publication 800-53 (Rev. 5): Security and Privacy Controls for Information Systems and Organizations.
4. Clarke, R., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.
5. Verizon. (2021). Data Breach Investigations Report (DBIR).
6. Symantec. (2021). Internet Security Threat Report (ISTR).
7. Cisco. (2021). Annual Cybersecurity Report.
8. The World Economic Forum. (2020). Cybersecurity Leadership Principles: Effective Leadership, Vision and Strategy for Cyber Resilience.
9. Microsoft Security Intelligence Report. (Retrieved from Microsoft's Security Intelligence Report archives).
10. The Center for Internet Security (CIS) Controls. (Retrieved from the CIS website).
11. Kaspersky Lab. (2021). Kaspersky Security Bulletin: Statistics of the Year.
12. Cybersecurity and Infrastructure Security Agency (CISA) Publications. (Retrieved from the CISA website).
13. Ponemon Institute. (2021). Cost of a Data Breach Report.
14. ENISA Threat Landscape Report. (Retrieved from the European Union Agency for Cybersecurity website).
15. US-CERT Alerts and Tips. (Retrieved from the Cybersecurity and Infrastructure Security Agency website).
16. CyberArk. (2021). Global Advanced Threat Landscape Report.
17. The National Cyber Security Centre (NCSC) Publications. (Retrieved from the NCSC website).
18. FireEye. (2021). Mandiant M-Trends: Threat Intelligence Trends and Insights.
19. McAfee. (2021). Threats Report.
20. Europol Internet Organised Crime Threat Assessment (IOCTA). (Retrieved from Europol's website).