PSG COLLEGE OF ARTS & SCIENCE

An Autonomous College- Affiliated to Bharathiar University
Accredited with A^{++} Grade by NAAC (4th Cycle)
College with Potential Excellence (Status Awarded by the UGC)
Star College Status Awarded by DBT – MST
An ISO 9001:2015 Certified Institution
Coimbatore – 641014

INTERNATIONAL CONFERENCE PROCEEDINGS ON EMERGING TRENDS IN TECHNOLOGY AND DIGITAL TRANSFORMATION FOR SUSTAINABLE BUSINESS DEVELOPMENT

Organised by
Department of Commerce with Computer Applications

Editors

Dr.M.Thirumagal Vijaya
Dr.D.Anandhi
Dr.G.R.Rajalakshmi
Dr.M.Rajakrishnan

29 JAN 2025

PSG College of Arts & Science

An Autonomous College- Affiliated to Bharathiar University
Accredited with A^{++} Grade by NAAC (4th Cycle)
College with Potential Excellence (Status Awarded by the UGC)
Star College Status Awarded by DBT –MST
An ISO 9001:2015 Certified Institution
Coimbatore – 641014

29 January, 2025

INTERNATIONAL CONFERENCE PROCEEDINGS ON EMERGING TRENDS IN TECHNOLOGY AND DIGITAL TRANSFORMATION FOR SUSTAINABLE BUSINESS DEVELOPMENT

Organised by

DEPARTMENT OF COMMERCE WITH COMPUTER APPLICATIONS

Editors

Dr.M.Thirumagal Vijaya

Dr.D.Anandhi

Dr.G.R.Rajalakshmi

Dr.M.Rajakrishnan

Multi Spectrum Publications

www.multispectrum.org

Edition: First

Year: January, 2025

ISBN: 978-81-984393-2-1

Publisher

(International Publisher)
Kanyakumari,Tamilnadu,India.
Phone: +91 6384730258
E-Mail: editor@multispectrum.org
www.multispectrum.org

CYBER SECURITY THREATS AND MITIGATION STRATEGIES FOR DIGITAL TRANSFORMATION

Dr. E. Renuga
Assistant Professor, Department of Commerce (Finance)
NGM College, Pollachi

Dr. G. Akilandeswari
Associate Professor & Head, Department of Commerce (Finance)
NGM College, Pollachi

ABSTRACT

Cyber security protects computer systems, networks, and data from unauthorised access, damage, or theft in the digital world. It involves measures and technologies designed to safeguard information and prevent malicious activities. Cyber security continues to be a top priority for businesses as cyber threats pose significant risks to their data and Experion's cutting-edge cybersecurity solutions empower them to protect their digital assets, ensuring a secure transformation journey while minimizing operational risks. Threat mitigation in cyber security involves identifying, analyzing, and implementing measures to minimize the impact of potential cyber threats, aiming to safeguard digital assets and systems against malicious activities such as hacking, data breaches, and malware infiltration.

Keywords: ***Cyber security, Technologies,*** *Threat, Mitigation.*

INTRODUCTION

The phrase "digital transformation" has come to connote creativity, effectiveness, and expansion in today's corporate environment. Digital technologies are being used by businesses in a variety of sectors to improve customer experiences, expedite procedures, and obtain a competitive advantage. But when companies go through this digital transformation, cybersecurity becomes a major worry. Cybersecurity and digital transformation services interact in a complicated way that necessitates careful consideration and strategic planning. Strong cybersecurity protections may not be given enough consideration by a product engineering team whose primary goal is to deliver the product on time. Understanding the requirements necessary for a new product or service's success, security, and size becomes crucial while developing it.

Cybersecurity aims to ensure data and systems' confidentiality, integrity, and availability, keeping them safe from unauthorised access, manipulation, or disruption. Techniques like encryption, firewalls, antivirus software, and user authentication are used to establish barriers and secure digital assets from potential risks.

By implementing effective cybersecurity measures, individuals and organisations can minimise the chances of cyberattacks and protect sensitive information from falling into the wrong hands.

The digital world is growing at an exponential rate, so fast that is difficult to comprehend how to counter the growing shadow world of cybercrimes. According to Statista, the global indicator 'Estimated Cost of Cybercrime' in the cybersecurity market was forecast to continuously increase between 2023 and 2028 by in total 5.7 trillion U.S. dollars (+69.94 percent). After the eleventh consecutive increasing year, the indicator is estimated to reach 13.82 trillion U.S. dollars and therefore a new peak in 2028. Currently in 2024, it is at 9.22 trillion dollars. Notably, the indicator 'Estimated Cost of Cybercrime' of the cybersecurity market was continuously increasing over the past years. However, even in the various types of attacks, there are definite patterns followed. Cyberattacks are steps, activities or actions performed by individuals or an organization with a malicious and deliberate motive to breach information systems, computer systems, infrastructures or networks.

Digital transformation is a complete shift that alters how companies function, provide value, and engage with stakeholders. It is not only about implementing new technologies. Among the pillars of this revolution are cloud computing, big data analytics, artificial intelligence (AI), and the Internet of Things (IoT). These technologies let businesses to automate processes, collect and analyse enormous volumes of data, and make decisions based on that data.

The foundation of any effective organisational change is digital transformation services. It includes a variety of services, such as data analytics, process reengineering, software development, and technology consultancy. Businesses can find inefficiencies, implement new tools, and optimise operations by utilising these services. But there are drawbacks to these adjustments, especially when it comes to cybersecurity.

IMPORTANCE OF CYBERSECURITY IN DIGITAL TRANSFORMATION

Four areas are commonly used to categorise digital transformation: domain, business model, process, and organization/culture. As a result, it naturally produces a deluge of connections and data. Although this abundance of data opens up new avenues for innovation and optimisation, it also exposes businesses to cyberthreats and data breaches.

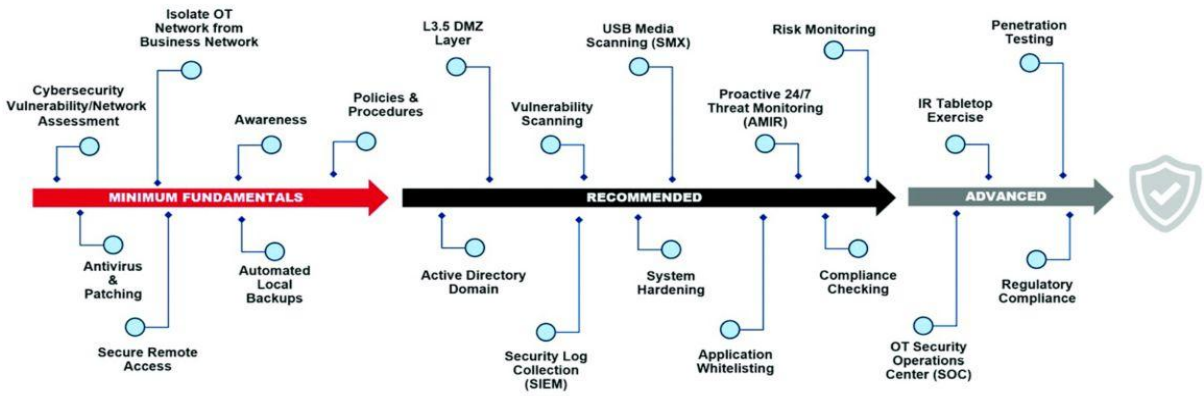
Any new technology plan must therefore be considered both a strength and a weakness. Before digital transformation can be properly implemented, organisations must take the time to develop a strong cybersecurity foundation that takes into account everything from legacy to high-tech assets and from existing to new IT infrastructure in order to preserve return on investment, reputation, and consumers.

The basic technology used by OT and IT are comparable. However, in the past, advancements have frequently been carried out independently, creating knowledge silos and new danger points. Integrating IT and OT is known as IT/OT convergence, and it is a crucial aspect of the Fourth Industrial Revolution. OT systems adjust business and industry activities and monitor events, processes, and equipment, whereas IT systems are utilised for data-centric computing. To put it briefly, IT/OT convergence is the process of integrating IT and OT systems. It makes it possible for them to exchange data in order to take advantage of this connectivity and raise the systems' worth. As a result of the growing dependence on computer systems,

web-based networking protocols, and the quantity of smart devices that comprise the internet of things, OT cybersecurity is becoming more and more significant.

OVERCOME CYBERSECURITY CHALLENGES DURING DIGITAL TRANSFORMATION

Cybercriminals have launched a series of highly coordinated and significantly more sophisticated cyberattacks in the last 12 months. According to cybersecurity data, 54% of organisations have already encountered an industrial control system problem. OT networks are being specifically targeted by cybercriminals. According to statistics, ransomware assaults against the manufacturing sector have increased by 156%, and 81% of malware has the ability to interfere with industrial control systems.
With new cyber threats emerging daily, the threat landscape is changing at an alarming pace. Appropriate action is no longer optional and must be implemented with a sense of urgency.



Because of its technical and political complexity, cybersecurity is one of the biggest problems the world is currently facing. The amount and calibre of data gathered, examined, and applied to lower business risk are directly tied to the capacity to carry out a robust cybersecurity response. Businesses are investing in OT cybersecurity with technology providers like Honeywell because they recognise that the future is unpredictable and want to be able to resist the most recent threats to their operations and come out stronger.

THREATS AND RISKS TO CYBERSECURITY

In the ever-evolving world of cybersecurity, there are several threats and risks that we need to be aware of. Let's dive into a few of them.

Malware Monsters

One of the biggest threats is malware, which includes viruses, worms, and ransomware. These sneaky little monsters can infect your devices and wreak havoc by stealing your data, encrypting your files, or even taking control of your device.

Phishing Pirates

Beware of phishing attacks! These are like deceptive messages from cyber pirates trying to trick you into revealing sensitive information, such as passwords, credit card details, or personal data. They often disguise themselves as trustworthy entities like banks or well-known companies.

Weak Castle Walls

If your devices or networks have weak security settings or outdated software, you open the castle gates for cyber intruders. They can exploit vulnerabilities in your systems and gain unauthorised access to your sensitive data.

Internet of Things (IoT) Troubles

The IoT poses new risks with the increasing number of interconnected smart devices. Insecure IoT devices can be gateways for cyber attackers to infiltrate your network, access personal information, or even control connected devices like cameras or thermostats.

Insider Threats

Not all threats come from external sources. Insider threats involve individuals within an organisation who misuse their access privileges or intentionally steal or leak sensitive data. It could be a disgruntled employee or someone who has fallen victim to social engineering tactics.

These are just a few examples of the threats and risks that cybersecurity faces today. To protect yourself digitally, it's important to stay vigilant, keep your devices and software up to date, use strong passwords, be cautious with suspicious emails or messages, and educate yourself about best cybersecurity practices. Enrol in cyber security courses online or cyber security certifications to learn more about the threats to digital assets.

MITIGATION STRATEGIES

Companies adopt various mitigation strategies to prevent cyberattacks and protect their sensitive data and systems. Some common strategies include:

Strong Perimeter Defense: Companies employ firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and control incoming and outgoing network traffic. These defences prevent unauthorised access and help identify and block potential threats.

Secure Network Architecture: Implementing secure network architectures, such as network segmentation and access controls, helps limit attackers' lateral movement within the network. This ensures that damage can be contained even if one part of the network is compromised.

Robust Authentication and Access Controls: Strong authentication mechanisms, like multi-factor authentication (MFA) and password policies, are enforced to prevent

unauthorised access to systems and sensitive data. Access controls are implemented to ensure that employees only have access to the information necessary for their roles.

Regular Patching and Updates: Companies maintain a proactive approach to patch management and software updates. They ensure that all software, operating systems, and applications are regularly updated with the latest security patches to address known vulnerabilities.

Data Encryption: Companies employ encryption techniques to protect sensitive data at rest and in transit. Encryption helps ensure that even if data is intercepted or stolen, it remains unreadable and unusable without the decryption keys.

Continuous Monitoring and Threat Intelligence: Companies employ security monitoring tools and techniques to detect and respond to potential threats in real time. They also leverage threat intelligence sources to stay informed about the latest threats and vulnerabilities, allowing them to implement preventive measures proactively.

Regular Security Assessments: Companies conduct periodic security assessments and penetration testing to identify vulnerabilities and weaknesses in their systems. These assessments help uncover potential entry points for attackers and provide insights for improving security measures.

By implementing a comprehensive approach that combines technical safeguards, employee awareness, and proactive measures, companies can significantly reduce the risk of cyberattacks and protect their valuable assets.

REDUCING CYBERSECURITY RISKS DURING DIGITAL TRANSFORMATION

Assess application architectures and underlying code regularly: Third parties that supply applications, such as EHR vendors and medical device manufacturers, should be held to strict information security and data protection standards and regularly assessed for new risks.

Control networks: Tightly and continuously monitor networks for evidence of suspicious traffic. In particular, network security and access controls should be used to prevent unauthorized access to health care critical infrastructure and critical software, especially legacy systems that cannot be easily patched or securely configured by default.

Conduct regular testing.

Identify gaps in security controls with regular vulnerability scanning and penetration tests against critical systems. This enables immediate remediation efforts before attackers can exploit the same weaknesses. Penetration tests should have explicit rules of engagement so as not to cause inadvertent outages to production systems and follow the tactics of known adversaries that attack health care providers.

CONCLUSION

Cybersecurity has become a crucial aspect of overall digital well-being. Companies and individuals must protect their information from cybercriminals. Digital transformation has

resulted in rapidly changing business environments that offer countless opportunities for innovation. With innovation, there will be additional risks. Strobes is a one-stop solution for all security stakeholders, ensuring that the business is well-guarded against technical issues and security threats. Whether it's your web application, mobile app, API, cloud instance, host, or network component, Strobes supports your investments, acting as an all-round security solution that ensures comprehensive risk mitigation.

REFERENCE

- https://timespro.com/blog/cybersecurity-in-the-era-of-digital-transformation-protecting-your-business
- https://strobes.co/blog/mitigating-the-risks-of-digital-transformation/
- https://timespro.com/blog/cybersecurity-in-the-era-of-digital-transformation-protecting-your-business
- https://www.balbix.com/insights/what-is-cyber-risk-mitigation/