iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 6 **Issue:** II **Month of publication:** February 2018

**DOI:**

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor : 6.887*
*Volume 6 Issue II, February 2018- Available at www.ijraset.com*

# Cyber Insurance Reduce Cyber Risks

Srinivas katkuri1
[1]*Research Scholar (UGC-NET in Law) Faculty of Law/University College of Law, Osmania University, Hyderabad-500007*

***Abstract:*** ***Cyber insurance is one of the most important new insurance lines to emerge in decades. It has been noticed that cyber crime costs organizations an estimated $400 billion every year, and this number is growing every year. Not surprisingly, cyber risk has emerged as one of the top risks that entering the market with cyber insurance policies. Cyber-insurance is enormously beneficial in the event of a large-scale security incident. Insurance provides a smooth funding mechanism for recovery from major losses, helping businesses to return to normal and reducing the need for government assistance. At a time when cyber threats are on the rise for banks for increasing cashless transactions and effects of demonetization, insurers see rise in demand for cyber insurance and cyber liability insurance, in particular. According to insurers there are various cyber insurance covers available in the country, but it is the cyber liability insurance which is in maximum demand for the banks. Cyber risk is now a major threat to businesses. Companies increasingly face new exposures, including first-and third-party damage, business interruption and regulatory consequences. With the operating environment for many industries changing dramatically, as they become more digitally-connected, this report examines cyber risk trends and emerging perils around the globe. It also identifies future mitigation strategies, including the role of insurance. Cyber insurance itself is not a defense. It's the application of cyber insurance as another layer of defense, complementing the efforts of IT and other information security functions, where the greatest value is realized. This paper explores about need of Cyber Security Insurance in India in this digitalization era especially in keeping centre point as digital cash or cashless transactions.***

***Keywords: Cyber risk, Cyber insurance, Cyber Security***

## I. INTRODUCTION

Technology has transformed the way business is conducted from providing services online to customers, to storing data in the 'cloud' while accessing information to large and small businesses alike. It also brings risk.[1] Individuals can suffer identity theft and fraud when compromised as a result of a data breach. They can also suffer embarrassment and distress when personally identifying information is publicly revealed. Whilst most information such as credit card details which can easily be turned into money, there are also a vast number of breaches that seek an organization's intellectual property.[2]

The last decade saw the introduction of digital and mobile banking facilities such as mobile wallets, net-banking, NEFT, RTGS and banking applications for convenience. With demonetization, the use of plastic and digital money has increased exponentially, making it a lucrative opportunity for sophisticated attackers to steal money by employing various tactics relating to different modes of payments. With the nudge to move to a cash less society, various digital payments platforms, wallets etc. are being used extensively by individuals for the smallest of transactions. Therefore, cyber attackers will look to finding new ways to exploit the situation by targeting individuals and digital payment service providers. This may be done by exploiting technical and process loopholes as well as lack of user awareness around the do's and don'ts.[3]

Recent Wanna Cry is a type of ransom ware, or extortive malware, that encrypts files, disks and locks computers.[4] Ransom ware is a malware that encrypts contents on infected systems and demands payment in bitcoins. It spreads laterally between computers on the same LAN by using a vulnerability in implementations of Server Message Block (SMB) in Windows systems. It also spreads through malicious email attachments. This exploit is named as ETERNALBLUE.[5] Wanna Cry is a type of ransom ware, or extortive malware, that encrypts files, disks and locks computers. The malware demands a ransom of ~$300-600 to be paid to one of three bitcoin accounts within three days in return for decrypting the files. WannaCry spreads via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network. Once successfully installed, this ransom ware scans for and propogates to other at-risk devices. WannaCry checks to see if backdoors (like Double Pulsar) are already on previously infected machines. Both Double Pulsar and the Eternal Blue exploit the SMB vulnerability that was made public by the Shadows Brokers hacking group in April 2107. [6]

There are approximately 30–40 publicly named companies among the likely thousands that were impacted by this ransom ware. Examples include the Russian Interior Ministry, Telefonica (Spain's largest telecommunications company) and FedEx. The UK National Health Service (NHS) was badly hit, with 16 of the 47 NHS trusts being affected, and routine surgery and doctor

©IJRASET (UGC Approved Journal): All Rights are Reserved

appointments being canceled as the service recovers. There are reports that in China over 40,000 organizations have been affected, including over 60 academic institutions.[7]

The initial vector of delivery for this malware was originally widely reported to be phishing emails, however data to validate this has not been confirmed and other reports suggest other vectors, such as the use of public-accessible vulnerable SMB (Server Message Block) to spread the malware in a worm-life fashion. Once an infection takes place, WannaCry beacons out to the kill switch URL in order to determine if the malware is in a sandbox environment. If the URL does not respond, then the malware starts to encrypt the victim's files using an AES-128 cipher. Files encrypted by WannaCry are appended with a file extension of .wncry as well as others. Unlike other ransomware families, WannaCry continues to encrypt victim files following any name changes and any new files created following infection. A ransom note is then displayed on the victim's machine, which is completed using text from a library of rich text format (RTF) files, in multiple languages and chosen based on machine location. Observed ransom demands require victims to pay either US$300 or US$600 worth of bitcoin (BTC) for a decryption key.[8]

## II. CONCEPT OF CYBER INSURANCE

At a time when cyber threats are on the rise for banks for increasing cashless transactions and effects of demonetization, insurers see rise in demand for cyber insurance and cyber liability insurance, in particular.[9] Cyber insurance is a tailor made insurance offering providing comprehensive cover for liability and expenses a business may incur arising out of unauthorized use of, or unauthorized access to, physical and electronic data or software within an organization's computer network or business. Cyber insurance policies can also provide coverage for liability, costs and expenses arising from network outages, the spreading of a virus or malicious code, computer theft or extortion. Traditional business insurance policies have tended to only cover "tangible" assets such as PCs, lap tops and other mobile devices.[10]

Cyber insurance also provides cover for business interruption and the cost of notifying customers and regulatory investigations or actions in case of a breach, without the requirement for physical damage that is a standard trigger under property policies. When looking at policy options, organizations should consider coverage which addresses these issues.[11]

## III. NEED OF CYBER INSURANCE

While insurance policies may help business recover some costs after-the-fact, they do not reduce cyber risks. Such risks are constantly evolving, along with technology, security vulnerabilities, and the motivations of cyber criminals. And individual industries are subject to specific risks based on their preferred technologies, the type of data they collect and store, and the potential impact of business interruption and property damage.[12]

Growth in the cyber insurance market has recently occurred at warp speed, with more than 60 companies writing in the United States alone.[13] The impressive year over year growth is expected to continue into the foreseeable future, with a variety of estimates placing market premium between $7.5 billion[14] and $20 billion by the end of 2020.[15]

This impressive premium growth is due to several factors; perhaps most notably, reporting of the various types of cyber attacks in the news on a regular basis, driving both awareness and fear. Not surprisingly, cyber risk has become a board-level concern in today's increasingly connected world.[16] On the surface, the cyber realm poses threats vastly different from what we've seen in other lines of business. Take geography, for instance. We are used to thinking about the impact of geography as it pertains to policyholder concentration within a specific region. It's well understood that within commercial property insurance, writers should be careful with respect to how much premium they write along the coast of Florida, as a single large hurricane or tropical storm can otherwise have an absolutely devastating effect on a book of business.[17]

Most large financial institutions in the U.S. typically purchase standalone cyber insurance coverage with limits between US$150 and $250 million, while some of them buy coverage on a blended basis (financial institution bonds and/or professional liability) with limits in excess of $250 million. Smaller institutions and non-traditional buyers in other industries are now following suit.[18]

Most cyber insurance policies do not cover bodily injury or property damage resulting from a cyber attack because, generally speaking, these risks have traditionally been covered (or not excluded) by Property & Casualty (P&C) policies and have not been well understood by the underwriting community. But the latest technology advancements in this industry are sparking a greater need for cyber insurance policies to provide affirmative coverage for bodily injury and physical damage or visa versa. When purchasing cyber insurance, look for underwriters and brokers who understand your specific industry sector, as well as the product. Industries are structured into vertical silos, but cyber is a horizontal phenomenon. While most cyber insurance products tend to be brokered and underwritten within the Errors & Omissions sector, it is really important to find a team that also has a solid understanding of P&C.[19]

©IJRASET (UGC Approved Journal): All Rights are Reserved

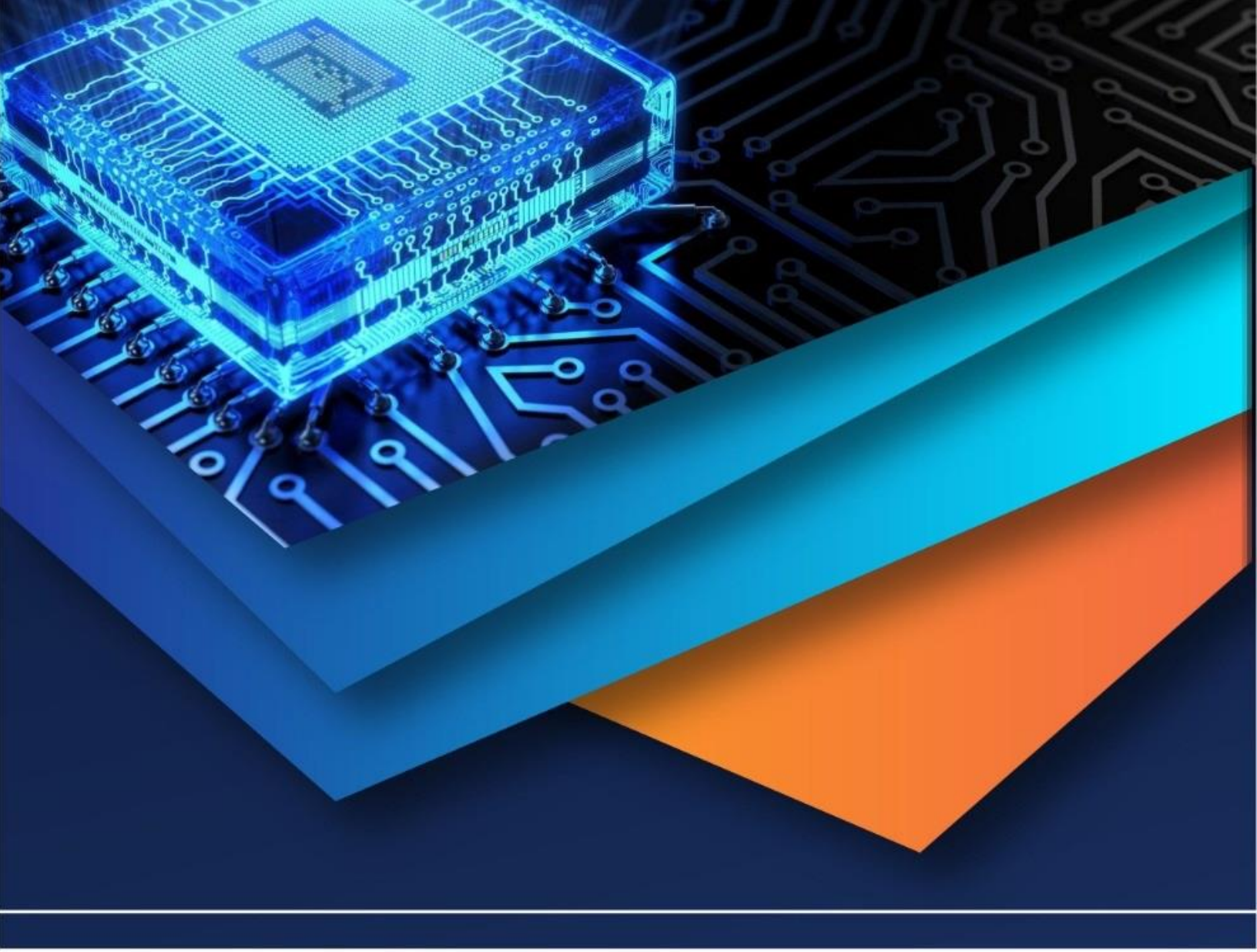
## IV. CONCLUSION

Cyber threats come in many forms—from external hackers bent on disrupting, damaging or stealing to well-intentioned employees unknowingly exposing personal or sensitive client information. Each organization must understand its own unique vulnerabilities. Recent high-profile attacks on retailers, banks and manufacturers underscore this point. There are likely many more unreported incidences kept confidential because of the negative impact of disclosure on reputation. In other cases, many organizations may not even know they've been breached. [20] Over the coming days and weeks, we anticipate that cyber criminals will release malware variants that leverage other and newer exploits, especially once more organizations patch systems to prevent EternalBlue. We expect that there could be more weaponization of the NSA's exploits that were leaked by Shadow Brokers. [21] Cyber insurance can come in a variety of forms, insuring companies for a wide range of risks, from reputational damage to theft of intellectual property. Some carriers also offer liability protection, including first party, third party, worldwide, business interruption, and network and information security protection, as well as security breach services, remediation and managed security services. Cyber insurance is still an emerging market, with significant variation in coverages and premiums from insurer to insurer. At the heart of this variation are differences among insurers in their ability to accurately assess policyholders' cyber risks and to respond appropriately to claims.[22]

## REFRENCES

[1] Cyber Insurance Research Paper, Centre for Internet safety, Sponsored by American International Group, Inc. (AIG)
[2] Ibid.
[3] "Responding to cybercrime incidents in India" A report by Fraud Investigation & Dispute Services (This report is prepared by the Fraud Investigations & Dispute Services team of EY in India.)
[4] WannaCry" ransomware attack Technical intelligence analysis May 2017, Ernst & Young Global Limited, a UK company
[5] Critical Alert Wannacry / Wanna Crypt Ransomware, Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics and Information Technology, Government of India
[6] "WannaCry" ransomware attack Technical intelligence analysis May 2017, op.cit.
[7] Ibid.
[8] Ibid.
[9] "Banks rush to buy cyber security cover as digital payments rise" PTI Feb 12, 2017, 04.23 PM IST, Mumbai, http://timesofindia.indiatimes.com/business/india-business/banks-rush-to-buy-cyber-security-cover-as-digital-payments-rise/articleshow/57109647.cms accessed on 22.05.2017 @12.45 p
[10] Cyber Insurance Research Paper, op.ci
[11] Cyber Insurance Research Paper, op.cit
[12] Pascal Millaire,John Farley, Sarah Stephens, Stuart Kohn,Paul Nikhinson,Mary Guzman,Sudhir Bhatti, "Latest Industry Trends in Cyber Security and Cyber Insurance" Symantec Corporation, 2016 http://images.mktgassets.symantec.com/Web/Symantec/%7B67fb9707-5ef8-4e90-b82b 8b3752d1dee6%7D_Latest_Industry_Trends_Cyber_Security_Insurance.pdf?aid=elq_&om_sem_kw=elq_16106716&om_ext_cid=biz_email_elq_(last accessed on 22.05.201
[13] Susanne Sclafane, "Cyber Risk Insurers Lag in Buying Cyber Cover", http://www.insurancejournal.com/magazines/features/2015/09/07/380313.htm, September 7, 2015.
[14] Matthew Heller, "Cyber Insurance Market to Triple by 2020", http://ww2.cfo.com/risk-management/2015/09/cyber-insurance-market-triple-2020/, September 15, 2015
[15] "Fitch" U.S. Insurers Writing Cyber Coverage Totaling $1B in Premiums", http://www.claimsjournal.com/news/national/2016/09/01/273172.htm, September 1, 2016.
[16] oshua Pyle, "Actuaries Beware Pricing Cyber Insurance is a Different Ballgame" http://images.mktgassets.symantec.com/Web/Symantec/%7Bc7498d04-a437-48a8-bbe3-f1486182a63c%7D_Symantec_Whitepaper_Actuaries-Beware-Pricing-Cyber-Insurance-20170110.pdf?aid=elq_&om_sem_kw=elq_16106716&om_ext_cid=biz_email_elq_ last accessed 22.05.2017
[17] Lynne McChristian, Hurricane Andrew and Insurance "The Enduring Impact of an Historic Storm", http://www.iii.org/sites/default/fles/paper_HurricaneAndrew_fnal.pdf, August 2012
[18] Pascal Millaire,John Farley, Sarah Stephens, Stuart Kohn,Paul Nikhinson,Mary Guzman,Sudhir Bhatti, "Latest Industry Trends in Cyber Security and Cyber Insurance" Symantec Corporation, 2016 http://images.mktgassets.symantec.com/Web/Symantec/%7B67fb9707-5ef8-4e90-b82b 8b3752d1dee6%7D_Latest_Industry_Trends_Cyber_Security_Insurance.pdf?aid=elq_&om_sem_kw=elq_16106716&om_ext_cid=biz_email_elq_(last accessed on 22.05.2017)
[19] Ibid
[20] CGI Cyber Risk Advisory and Management Services for Insurers Minimizing Cyber Risks, CGI (CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and managed services.
[21] "WannaCry" ransomware attack Technical intelligence analysis May 2017, Ernst & Young Global Limited, a UK company
[22] CGI Cyber Risk Advisory and Management Services for Insurers Minimizing Cyber Risks, CGI (CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and managed services.)

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)