PRIME INDEXES

WHITEPAPER

Cybersecurity Industry Overview

www.primeindexes.com

Contents

Introduction

The digital age is now well upon us, and we live in an era where cyberspace has become indispensable for our everyday activities. The digital form has entered all aspects of our lives – shopping, entertainment, banking, and so on. Without a doubt, these advancements have made our lives easier. However, our increasing reliance on cyber infrastructure makes us more vulnerable to cyberattacks. According to University of Maryland's Clark School of Engineering, a cyber-attack occurs every 39 seconds, affecting one in three Americans each year.[1,2] To fully benefit from the digital era, we need to feed it data, including our personal data, which could cause severe harm if it falls in the hands of a hacker.

While as individuals, it is important to ensure our personal data is protected, the impact of a data breach on a corporation can be far-reaching. The firm can lose its intellectual property, trade secrets, and most importantly, hard-earned customers and stakeholders. Problems do not end there – the company could also come under regulatory scrutiny from a number of agencies (such as the Federal Bureau of Investigation, Secret Service, Immigration, and Customs Enforcement) and could be held answerable to regulators including State Attorneys General, the Federal Trade Commission (FTC), and the Securities and Exchange Commission (SEC).[3]

A cyber breach can take place from any country at any point of time, making this threat all the more menacing. How do we protect ourselves against enemies we cannot see or hear and do not even know of? The answer lies in creating an effective cybersecurity program and structure. Cybersecurity aims to protect systems, networks, and programs from digital attacks.[4] Given the complexity of different forms of data storage, and the number of devices we use, it has become particularly challenging to develop the right cybersecurity strategy as attackers continue to innovate. The concerns about cyber-attacks have become greater than ever before thanks in part to the reported attempts made by hackers to influence the 2016 U.S. presidential election.[5]

Evolution of Cybersecurity

The words “hacking”, “virus,” and “data breaches” ring alarm bells today, but they had humble beginnings back in the 1970s. The first known digital virus was popularly called “the creeper.” An engineer from US technology company BBN Technologies created a code for a program that could travel from one computer to another connected by the advanced research projects agency network (ARPANET) – the Internet’s predecessor.

The virus did not particularly inflict much damage other than causing slight inconvenience to the reader. It would display the message “I’m the creeper, catch me if you can!” In response, his colleague wrote another code, which went one step ahead, as the code would not just move between systems but also copy itself as it traveled. This program would delete the creeper message, thus earning the name “reaper.”[6]

The Morris Worm

In 1988, the first major cyberattack in the form of distributed denial-of-service (DDoS)[7] attack occurred, affecting reportedly 6,000 computers. The Morris worm, written by a university student significantly slowed the computer it infected. It could also affect a single computer multiple times, slowing the computer each time until it crashed.[8] This pre-digital-era case is important owing to its sophisticated nature; the attack combined DDoS, exploits, stealth technologies, password brute forcing, and other techniques in bringing the Internet to a standstill. Although the worm was neutralized in about 48 hours, its impact was foreboding.[9]

Emergence of Computer Emergency Response Teams

The Morris Worm attack and the few others that followed led to the establishment of computer emergency response teams (CERTs). CERTs emerged as the first major players in the global cybersecurity industry. In the United States., US-CERT was set up under the supervision of the National Cybersecurity and Communications Integration Center (NCCIC) to promote faster data sharing and emergency situation reporting, and to reduce the possibility of cyber threats.[10] As the Internet evolved and expanded through the 1990s so did the threat of virus attacks. This led to the emergence of antivirus software, which was initially used to detect viruses and prevent them from causing damage. However, antivirus software continued to evolve and can currently identify and tackle not only viruses, but all external threats such as phishing, ransomware, and botnet attacks.

Cyberattacks in the Millennium

The Internet saw unprecedented growth in the 21st century and the threat of cyberattacks grew along with it. At this time, cybersecurity gained more prominence, as victims of cyberattacks included some of the world's top corporations[11] reiterating the need and urgency to create a cybersecurity strategy within the workplace.

TJX Companies Inc.: In 2007, TJX Companies Inc., a US multinational department store corporation, disclosed that a group of hackers had cracked its weak and outdated encryption standard and stole over 90 million credit card details. Interestingly, the hackers did not deploy any sophisticated tools, rather they used a powerful antenna to break into the wireless networks of two TJX stores. The collective economic damage to banks and insurers was estimated at around $200 million.[12,13]

Stuxnet: In 2010, a worm named Stuxnet attacked and infiltrated over 15 uranium enrichment facilities in Iran. Stuxnet is regarded as the world's first digital weapon designed specially to thwart Iran's nuclear program. Unlike other worms or viruses, it could cause physical destruction to equipment. According to estimates, around 984 Iranian uranium enrichment centrifuges were damaged by Stuxnet.[14,15]

RSA Security: In March 2011, RSA Security, a U.S. computer and network security company, reported that records of around 40 million employees had been stolen by two separate hacker groups that worked in collaboration with a foreign government to launch a series of phishing attacks. This incident sent shockwaves across the industry especially considering RSA was one of the biggest security vendors.

Target: Departmental store operator Target came under attack in late 2013, with the company reporting that personal identity information (including name, address, email address, and telephone number) of nearly 110 million of its customers had been compromised. Target's CIO resigned in March 2014. The cost of the breach was estimated at $162 million.

Yahoo: In 2014, Yahoo became the victim of the biggest data breach in history, which compromised the name, email address, date of birth, and telephone number of 500 million users. Later, Yahoo revised that estimate, claiming all 3 billion user accounts had been compromised. At that time, the company was in the midst of talks with Verizon for a potential sale. The attack is said to have knocked off an estimated $350 million from its valuation.

Ebay: Online auction company Ebay reported a cyberattack in May 2014, which compromised details of 145 million of its users. The hackers used the credentials of three company employees to gain access to the company's database for 229 days. Ebay reported none of the financial information was accessed, as it was kept separately. Nevertheless, the company received a lot of criticism for lack of communication to its users and its sloppy password renewal process thereafter.

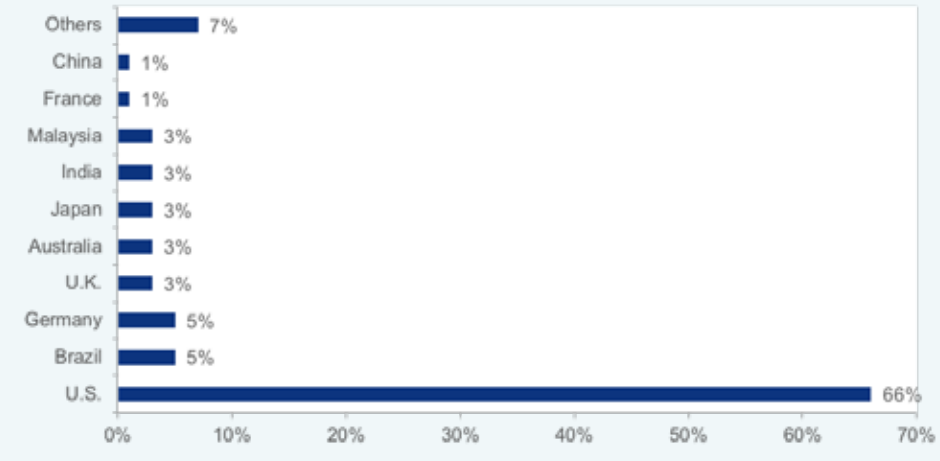
JP Morgan Chase: The U.S. multinational investment bank reported a security breach in 2014. Hackers managed to steal names, addresses, phone numbers, and email addresses of 76 million households and 7 million small business accounts. Allegedly, the hackers managed to get "root" privileges for over 90 bank servers, arming them with the ability to transfer funds. However, no money was stolen from the bank. Owing to the scope and magnitude of the breach, it was dubbed as the largest theft of customer data from a U.S. financial institution.[16,17]

WannaCry: A ransomware named WannaCry struck computers across 150 countries in 2017, taking control of infected computers by encrypting the contents of their hard drives. Once a system was encrypted, the hackers behind the ransomware demanded money to decrypt files. The severity of the attack could be gauged by the fact that it affected over 300,000 machines across numerous industries, including health care and automobile manufacturing. Surprisingly, it exploited a Windows vulnerability, which was allegedly discovered by the U.S. National Security Agency (NSA). Apparently, this vulnerability information was stolen from the NSA and leaked by a hacking group.[18,19]

Equifax: In 2017, consumer credit reporting agency Equifax reported that personal information of 143 million customers and credit card details of 209,000 customers had been stolen. The company stated later that as many as 147.9 million customers were affected. It was criticized in the U.S. Senate hearing for failing to keep its computer systems adequately up-to-date and not coming forward with the true description of the damage earlier.[20]

In its Cybersecurity Statistics report 2018, UK tech-analysis firm Comparitech stated the U.S. was one of the most targeted countries in cyberattacks.

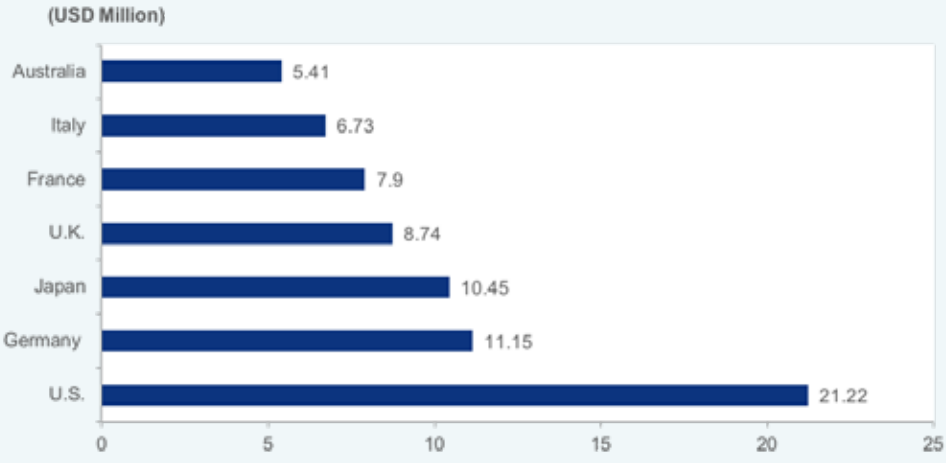
Most Targeted Countries for Web Application Attack Traffic



Source: Comparitech[21]

In terms of monetary losses due to cybercrime, the U.S. led all major economies as of August 2017, emphasizing the greater need to reduce the number of crimes.

Average Annualized Cost of Cyber Attacks Per Organization in Major Countries (FY 2017)



Source: Accenture, 2018[22]

Types of Cyberattacks

The various incidences of data breaches have taught us that data breaches and cyberattacks can take many forms and cause damage from any environment the systems are exposed to. For an institution to protect itself against digital attacks, it is important to know the areas of vulnerability and the impact of an attack so it can continue to update its cybersecurity policy to keep pace with the ever-evolving technological advancements.

Cyber threats can be grouped on the below – attacks on Integrity, Confidentiality, or Availability ("ICA") – the three pillars of cybersecurity.

Attack on Integrity

Integrity attacks indicate data have been tampered with or altered by unauthorized people. Consequences of an attack on integrity can be mild to severe, depending on the quantity of data stolen. Ensuring backups are available to retrieve affected data is an example of a precautionary measure to address this type of an issue.

Attack on Confidentiality

Theft of private or confidential information by an unauthorized person is an attack on confidentiality. This marks the start of a cyberattack, as it gives an unauthorized external party the right to access systems and databases and, hence, misuse the data.

Attack on Availability

Attacks on availability prevent an authorized person from accessing information or services that would otherwise be available to him/her. This type of attack is relatively common, with high-profile websites attacked by attackers, denying their users access to resources of the websites.[23]

Means of Cyberattacks

The means by which the above-mentioned cyberattacks are generally carried out are explained below.

Social Engineering

In this type of attack, an attacker does not target systems but people who work with the systems. For example, instead of trying to obtain data about clients by hacking into the systems of a company, the attacker may call up an employee, posing as a client to extract privileged information.

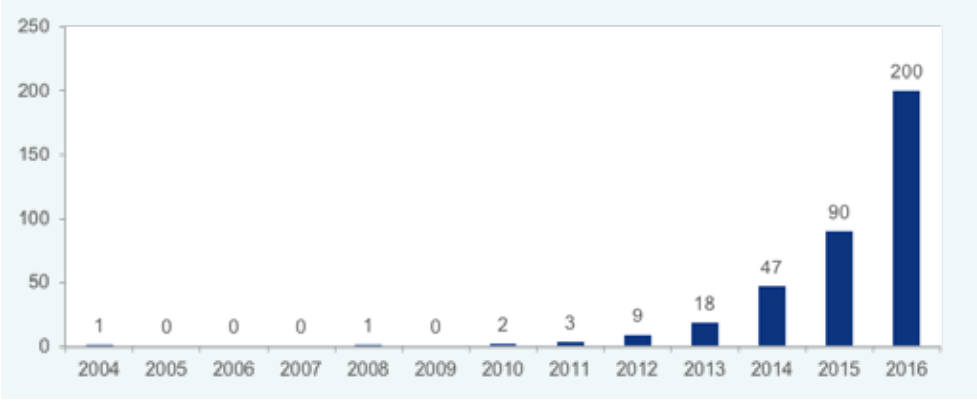
Phishing

In another form of attack targeting humans, hackers use misleading emails to trick employees and obtain details. This is one of the most widespread cyber threats, with several firms falling prey.

Ransomware

Ransomware is a type of malicious software that threatens to harm a system by denying the user access to data, unless a ransom is paid. Usually, the ransom quoted by an attacker tends to be a small amount so that the victim does not have to think twice about paying it. Some attackers even go to the extent of offering early bird discounts so the victim is not tempted to resort to legal action. Researchers have found that the number of new named ransomware threat variants increased to 200 in 2016 from 3 in 2011.[24]

Number of New Named Ransomware Threat Variants



Source: Secureworks[25]

Unpatched Software

A company's failure to patch existing software can leave it exposed to vulnerabilities and attacks. Unpatched software constitutes one of the most serious cybersecurity threats for a company, as they lead to reputational and financial damage, with the company facing censure for negligence.

Social Media Threats

Hackers often create malicious and fake websites using URLs similar to famous social media platforms (such as Facebook or Twitter). This threat could be extremely dangerous, given a large number of users share abundant personal information in social media and their connections become easy targets once an account is hacked.

Advanced Persistent Threats

The purpose of the attacker in this case is not to cause disruption or immediate damage to the target, but gain access to systems to continuously monitor data and eventually steal it. Companies in intellectual-property-focused industries are usually the target of these attacks.[26]

Building a Cybersecurity Strategy

Cybersecurity seeks to protect the Integrity, Confidentiality and Availability (ICA) of information, and it forms the basis of a strategy to protect data against all forms and means of breaches.

An effective cybersecurity strategy should consider the following solutions.

Cybersecurity Risk Management

Owing to increasing dependence on digital infrastructure, businesses face a challenge in striking a balance between protection and progress, as well as privacy and governance. Governance risk and compliance challenges could arise from the inappropriate protection of digital assets, lack of optimization of compliance management tools, and absence of a proper compliance structure. Cybersecurity risk management involves identifying external/internal vulnerabilities in an organization's cyberspace and finding solutions to protect it. Risk management requires a detailed risk assessment, which involves the identification of technology gaps. An organization may have sophisticated cybersecurity tools; however, these tools may not necessarily address specific vulnerabilities. For instance, an organization may find through its external threat assessment that its employees are vulnerable to phishing scams. In such a situation, the organization should devote more effort to training its employees to refrain from opening attachments from unknown senders. Therefore, detailed organization-specific risk assessment ensures cybersecurity tools deployed by an organization are appropriate for the particular risks it faces. On top of proactive measures, businesses need to have a crisis management strategy to respond to any significant breach or theft of critical data. Risk management plays an important role in the overall growth, stability, and sustainability of an organization.[27,28,29]

Unified Threat Management

Unified threat management (UTM), as the name suggests, refers to a single security solution that provides multiple security functions at a single point on the network. A UTM appliance offers a comprehensive security package – antivirus, antispyware, antispam, network firewalling, intrusion detection and prevention, content filtering, and leak prevention. UTM appliances have gained traction, due to increasing blended threats – attacks that use combinations of different types of malware and launch attacks on separate parts of a network simultaneously. Preventing such attacks can be difficult if an organization uses separate appliances and vendors for each security task. By creating a single point of defense, UTM improves the ability to deal with various threats.[30,31,32]

Security Incident Management

Security incident management (SIM) involves dealing with security incidents (threats) in real time. Security incidents include policy violations, unauthorized access to data (health and financial data, and social security numbers), and crashing of servers. SIM helps an organization minimize the impact of a cyberattack and get back to business as soon as possible. It is a multifaceted strategy, combining appliances, software, and human-driven investigation. It usually starts with an alert about an incident, followed by the engagement of the incident response team consisting of representatives from various departments including legal, communications, finance, operations, and IT. Incident responders analyze an incident and develop a plan to remove any threats or issues. The biggest benefit of SIM is that it enables an organization to respond to threats systematically by following a consistent incident-handling methodology, thereby minimizing the impact of a disruption in services.[33,34,35,36,37]

Identity and Access Management

Cloud, mobile, and Internet of things (IoT) technologies allow businesses to enable employees to move beyond the protection of a firewall and work from any location. Even customers are able to interact with organizations through multiple channels. This has increased challenges relating to identity and access manage-

ment (IAM). IAM puts user identity at the center of the cybersecurity model. It is a crucial undertaking for any enterprise, as IAM products provide role-based access control tools, which help organizations regulate user access to critical information. Its core objective is to provide a digital identity to every user, whether it is a client or employee. Compromised user credentials are one of the major causes of security breaches. IAM mitigates this threat by providing single sign-on (access to multiple applications using one set of credentials), multifactor authentication (which combines two or more independent credentials), access management, and many more solutions. Implementing IAM and its best practices can provide an organization with significant competitive advantages. For instance, opening a network, without compromising security, to employees, clients, partners, and suppliers can improve efficiency and lower operating costs.[38,39,40,41]

Components of Cybersecurity Strategy[96]

Critical Infrastructure

Critical Infrastructure refers to physical and virtual systems, body of network, or assets essential for the smooth functioning of the economy including the electricity grid, traffic lights, and hospitals. The importance of the effective functioning of critical infrastructure is quite high thanks to the extent of damage failure of any of these systems can cause. If there is no resilient cybersecurity program in place, cyber terrorists could completely disrupt the economy, derailing economic growth. The need for cybersecurity in the critical infrastructure industry is at an all-time high, as many sectors use digital processes in place of manual ones.

Network Security

Network security refers to any activity designed to protect the usability and integrity of a network. It consists of multiple layers of defense intended to block unauthorized users and malicious insiders. These layers apply a combination of security controls to filter threats trying to penetrate a network. They are built through firewalls, intrusion prevention systems, and antivirus components. The firewall is considered the most important component, as it forms the base of network security.[42]

Cloud Security

As more enterprises continue to switch to the cloud, there is a greater need to set up cloud security. As cloud infrastructure is a shared environment, the threat to privacy and data protection requirements are high. Cloud security provides many functionalities of traditional IT security, but in the cloud infrastructure. These days, several cloud providers also offer security tools to enterprises to better secure their data.

Application Security

Application security, once considered an afterthought in designing an application, is at the forefront of software development. With the widespread awareness of and need for cybersecurity, many software applications are being introduced that have embedded features to shield an application from different forms of threats.

Internet of Things Security

IoT refers to the connection of physical objects we use in our everyday life via the Internet that helps in communication. Over the last few years, the IoT industry has gained traction; with many claiming it has the potential to change the way the world functions. The biggest threat to the IoT's growth is a cyber threat. IoT security aims to protect devices connected to a network and the network itself from external threats.

Layers of Cybersecurity

Hackers are always improving their means of unearthing flaws in computer networks. As highlighted above, 2017 witnessed a massive ransomware attack – WannaCry, which was the most sophisticated attack of its kind. Under such circumstances, the best way to protect cyberspace is by creating and deploying a multilayered security strategy.

Network Firewall

A firewall protects an organization against network-based attacks from hackers, viruses, and worms. It is the first line of defense, similar to walls built around medieval castles to restrict unauthorized entry. Firewalls monitor incoming and outgoing network traffic using predetermined rules. A firewall is an essential component of cybersecurity strategy and must be updated regularly to thwart emerging threats. It protects a network from a broad range of attacks such as DDoS, browser, and brute-force attacks.[43]

Physical Security

We secure our valuables by locking them in vaults, for example. One should give equal importance to physical security and monitoring of server rooms, desktops, and external hard drives. This could be done by installing surveillance systems, locking server rooms using finger print and facial recognition technologies, keeping track of mobile devices, and using password-enabled screen savers.[44,45,46]

Identification and Elimination of Loopholes

Organizations should seek the help of experts and identify vulnerabilities in their system. Most common vulnerabilities include weak passwords, outdated firewalls, missing software patches, unencrypted data, outdated antiviruses, unrestricted use of USB flash drives, and unsecured Wi-Fi networks. Once it is identified, the vulnerability must be addressed to mitigate any threats. Vulnerabilities can be fixed through regular system checks, vulnerability and threat scans, application of software patches, and firewall and antivirus/malware software updates.[47,48]

Data Encryption

Data encryption translates digital data into undecipherable code so that only authorized people with access to a decryption key (password) can access it. If a hacker manages to circumvent all network-based defenses, data encryption systems will act as the last layer of security. Interestingly, the encryption strength of a system is directly proportional to size and complexity of the key. Protection against brute-force attacks (where a hacker tries random keys until the right one is found) requires a long and complex key.[49,50]

Security Training

An individual is the most important element, but also the weakest link in the implementation of a cybersecurity strategy. It is entirely possible that a cybersecurity program, even when created to near perfection, can fail if the concerned person does not know how to operate it or take adequate defensive measures during an attack. For instance, many malware attacks have been successful because of someone's browsing unsolicited links or clicking on an affected email attachment. It is extremely important that every organization conducts basic training for all its employees so they are aware of what constitutes a data breach and how to tackle it.[51]

Business Continuity and Disaster Recovery

Business continuity and disaster recovery (BCDR) is a broad term that combines a set of processes and techniques to help an organization recover from a disaster. This aspect is often overlooked while developing a cybersecurity strategy. The outcome of data loss from natural disasters or cyberattacks can be severe for a business. About 25% of organizations that have faced cyberattacks lose significant business opportunities following the data-loss event.[52] BCDR involves identifying potential threats (such as cyberattacks, natural disasters, failure of IT systems, and fire) and preparing a continuity and recovery plan. Backups are an essential part of BCDR – a well-managed backup is highly effective against ransomware attacks.[53]

Latest Technological Developments in Cybersecurity

Blockchain

With the progress in technology and increased complexity in cyber protection, several companies are showing interest in blockchain as part of their cybersecurity strategy. Blockchain is a decentralized and digitized public ledger containing blocks of information or transactions linked to each other.

Some reasons for switching to blockchain technology are:

Decentralized: It is one of the main reasons why companies are contemplating using blockchain technology. Traditional databases are kept in a centralized location, making it easier to attack, as the coding is also concentrated in a single place. In the case of blockchain, when an unauthorized person tries to tamper with a block of data, the system checks each block to ascertain which one differs from the rest and simply discards this block from the chain if it finds out it is false.

Easily traceable and permanent: All transactions added to a blockchain are time-stamped and digitally signed. This makes it easier to trace the time period of the data and the authorized owner of the data. When new data is added, it only gets linked to the original data; hence, data in the blockchain is permanently available.[54]

No human errors: With blockchain technology, companies can authenticate users while avoiding a user-created password. This blocks a potential route to attack, as the need for login and password is eliminated. It also saves time for employees.

Artificial Intelligence

Artificial intelligence (AI) is the process of training machines to learn from experience so they can work, learn, and react like humans. This explains why several companies are keen to invest in AI in their attempt to counter cyberattacks.

AI can be used in cybersecurity in the following ways:

- AI can respond to cyberattacks. Tools that use AI can help organizations become more effective in combating cyberattacks by bridging the skills and resource gaps, thereby helping them identify and prevent cyber threats.[55]
- It can be used to identify vulnerable areas within different parts of a business and remediate errors within them. For instance, IBM's Watson for Cyber Security, an AI-powered computer system, is capable of learning from past cyberattacks, thereby enabling organizations to respond to threats at greater speeds.[56]
- According to Cisco Annual Cybersecurity Report 2018, AI can be used to automatically detect unusual patterns in encrypted web traffic and IoT environments.[57]

Regulatory Developments in Cybersecurity Space

Global Centre for Cybersecurity

In its Global Risk Report 2018, the World Economic Forum (WEF) listed cyber threat as one of the most critical risks threatening the world economy. In the same report, it reported cyberattacks would constitute the third-largest global threat, most likely over the next five years. In January 2018, the WEF announced plans to establish a Global Centre for Cybersecurity to provide a global platform to governments and corporations to work on cybersecurity challenges. The center is based in Geneva, Switzerland, and works under the WEF's supervision. It began formulating a comprehensive regulation for cybersecurity, influencing the creation of the General Data Protection Regulation (GDPR).[58,59]

General Data Protection Regulation

The GDPR, which came into effect on May 25, 2018, was implemented to establish a single set of rules applicable to all companies in the European Union (EU) and to protect the personal data of all EU citizens. In January 2012, the EU drafted a data protection reform across the EU, and in 2016, the European Parliament approved the draft of GDPR. Each organization within the EU, as well as organizations outside the EU that have customers in the EU, have to comply with the GDPR.[60]

The GDPR imposes strict punishment for noncompliance, with fines ranging from €10 million to 4% of the company's annual global turnover. Infringement of rights could cause a company a maximum fine of €20 million or 4% of its global turnover. In addition, a company also runs the risk of significant reputational damage, as organizations are obliged to report any breaches.

A major change brought about by the GDPR is the concept of breach notification. If a company's data is stolen, it is obliged to deliver a breach notification. The breach notification should be sent directly to each victim whose personal details were stolen. In addition, the breach must be reported to the member state's relevant regulatory body within 72 hours of the organization's becoming aware of it.[61]

The U.S. and Cybersecurity

The U.S. does not have a single all-encompassing data protection law or regulations such as the EU's GDPR. Rather, it regulates cyberspace through numerous privacy laws and regulations developed at the federal and state levels. The current regulatory structure for cybersecurity in the U.S. is a matrix of numerous laws that regulate the private sector, public authorities, financial institutions, health-care organizations, and third parties.

For the private sector, the Cybersecurity Enhancement Act of 2014 authorizes the National Institute of Standards and Technology (a non-regulatory agency of the U.S. Department of Commerce) to coordinate with the private sector and develop a comprehensive, voluntary, and consensus-based set of cybersecurity standards and best practices for businesses to manage and reduce cybersecurity risks. In addition, the Cybersecurity Act of 2015 establishes a voluntary framework for private entities, the federal government, and state governments to share real-time information on cybersecurity attacks. Most importantly, this act provides liability protection to private entities sharing information on cybersecurity risks with federal agencies.[62,63,64]

For public authorities, the National Cybersecurity Protection Act of 2014 directs the Department of Homeland Security (DHS) to collect and share information about cyber threats with the public and private sectors. Further, the Federal Cybersecurity Enhancement Act of 2016 and the Federal Information System Modernization Act of 2014 (FISMA 2014) authorize the DHS to play a leadership role

in administering the implementation of intrusion assessment plans for federal authorities.[65,66]

For financial institutions, the Gramm-Leach-Bliley Act of 1999 (GLBA) requires financial institutions to disclose their information-sharing practices to their clients and safeguard sensitive data. It also mandates financial institutions to grant their clients the right to not share their personal data with third parties. The GLBA is jointly enforced by the Federal Trade Commission, along with federal banking agencies and other federal regulatory authorities.[67,68]

Health-care organizations are regulated through the Health Insurance Portability and Accountability Act of 1996 (HIPAA). It is a set of standards established to secure protected health information (any information about health status) held or transferred in electronic form. The act specifies a series of administrative, technical, and physical security procedures to be followed to assure the ICA of protected health information. HIPPA is applicable to any health-care provider (including health-care clearing houses) that electronically transmits information related to health. Additionally, the Electronic Communications Privacy Act of 1986 prohibits third parties from unauthorized interception or disclosure of data related to communication.[69,70]

Current Regulatory Structure for Cybersecurity in the U.S. is a Matrix of Numerous Laws

Sector	Acts	Regulatory Authority
Private Sector	Cybersecurity Enhancement Act of 2014	United States Department of Commerce
	Cybersecurity Act of 2015	Department of Homeland Security
Public Authorities	National Cybersecurity Protection Act of 2014	Department of Homeland Security
	Federal Cybersecurity Enhancement Act of 2016	
Financial Institutions	Gramm-Leach-Bliley Act of 1999	Federal Trade Commission, federal banking agencies and other federal regulatory authorities
Healthcare Organization	Health Insurance Portability and Accountability Act of 1996	Department of Health and Human Services

Note: Table includes only major laws

The U.S. government is taking preliminary steps to create a set of nationwide data privacy rules similar to the GDPR. The National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce, has proposed a framework to protect consumer data and privacy online by creating a suite of nationwide data privacy rules. It has already held over 50 meetings with tech companies, Internet providers, and others. In its proposed framework, the NTIA has laid down goals related to the transparency, security, and control of personal data collected by these entities. It also proposes that organizations employ security safeguards for the protection of data and privacy. The agency has sought public input on these proposals. Interestingly, the State of California has recently passed the Consumer Privacy Act of 2018, which mirrors the EU's GDPR in several ways. The law gives Californian citizens the right to view, make corrections, and delete data held by companies operating in the state. Citizens will also have the right to prohibit companies from selling data to third parties. The law will come into effect by 2020.[71,72,73,74,75,76,77]

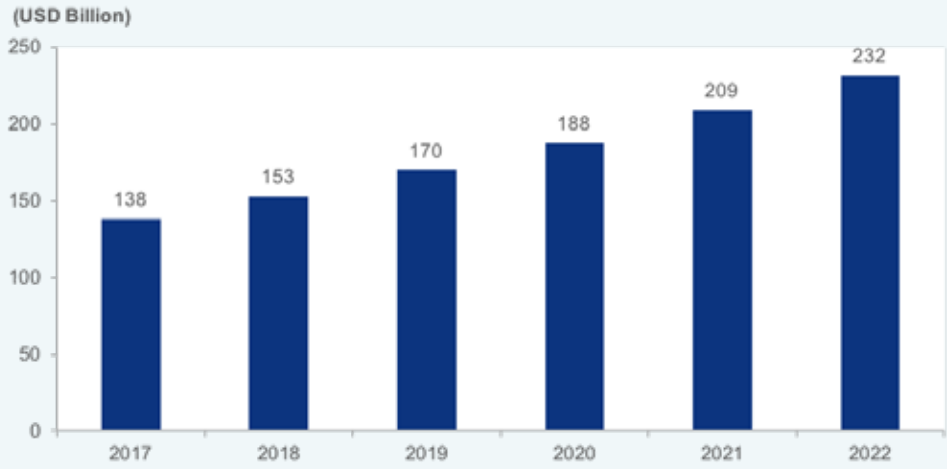
Australia – Australian Cyber Security Centre

The Australian government established the Australian Cyber Security Centre (ACSC) in 2014 to coordinate the country's cybersecurity operations and capabilities. ACSC pools the knowledge and resources of the country's five top organizations – Defence Department, Attorney-General's Department, Australian Security Intelligence Organization (ASIO), Australian Federal Police (AFP), and Australian Crime Commission.[78]

Cybersecurity: Industry Trends and Future Prospects

The global cybersecurity market grew from $3.5 billion in 2004 to about $138 billion in 2017 –over 39x in 13 years. In 2017, the aerospace and defense vertical had the largest share in the cybersecurity market. However, going ahead, government, BFSI and IT and telecom verticals are expected to gain traction. During 2017 to 2022, the cybersecurity market is expected to grow at a CAGR of 11% to reach $231.94 billion. North America dominated the global cybersecurity market in 2017, this trend is also expected to change as APAC is estimated to grow at the fastest pace during 2017-2022.[79,80,81]

Size of the Cybersecurity Market Worldwide



Source: Statista,2018[82]

Rise of IoT will require more sophisticated security solutions: The use of big data, autonomous vehicles, virtual assistants, cloud computing, and IoT/connected devices will increase our susceptibility to cyberattacks. However, cybersecurity will also evolve rapidly and create robust self-healing and self-defending networks by leveraging AI and blockchain. AI-based security solutions will increasingly be deployed by organizations to shore up defense and protect valuable data. Alphabet Inc. has already provided a promising solution. Chronicle, a security company (Alphabet's subsidiary) that uses AI-based solutions for the cybersecurity industry, claims to deploy planet-scale computing and analytics to fight cybercrime on a global scale.[83,84,85,86,87,88]

Cybercrime will evolve as a business: Cybercriminals will increasingly use more computing power and complex techniques, and threats such as phishing, mobile malware and ransomware will evolve and become more sophisticated. Amateur hackers are already changing their modus operandi, making it a professionally run business. Sophisticated attacks on critical infrastructure and supply chain will increase. This would give a big boost to the ethical hacking industry, which, in turn, would bolster the cyber security industry.[89,90]

Corporations will spend large amounts on cybersecurity: According to a global survey by Ernst & Young (2017-18), 87% of the surveyed organizations stated they required 50% more budget for cybersecurity. In another global survey, 78% of the organizations reported that they plan to increase cybersecurity budget in 2018; the percentage for the US was higher at 86%. Many global corporations have already announced increased cybersecurity budgets. JPMorgan Chase has doubled its annual cybersecurity budget to $500 million from $250 million. The Bank of America stated it had an "unlimited budget" to combat cybercrime.[91,92]

Cyber defense will become an integral part of a nation's defense budget: Apart from cyberattacks on businesses, state-sponsored attacks will also increase going ahead. States will develop sophisticated cyberattack technologies for both defense and offense, and the budget for cyber defense will become an integral part of the overall defense budget of a nation. The US government allocated $19 billion for cybersecurity as part of its 2017 budget, a sharp increase from $14 billion in 2016. Australia has a projected investment of over $230 million over the next four years, which is significant compared to its defense expenditure of $400 million during the same period.[93,94]

Cybersecurity will emerge from a niche profession: The cybersecurity space will also witness the evolution of new professions and domain expertise. It is estimated that about 3.5 million new cybersecurity jobs will be created by 2021. The French Ministry of Defense has declared its plans to create 450 jobs in 2019, 75% of which will be devoted to cyber security and intelligence.[95]

References

1 https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

2 https://www.cybintsolutions.com/cyber-security-facts-stats

3 https://www.csoonline.com/article/3261405/leadership-management/corporate-boards-will-face-the-spotlight-in-cybersecurity-incidents.html

4 https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

5 https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable

6 https://www.techly.com.au/2018/02/14/techly-explains-fascinating-evolution-cybersecurity

7 A DDoS attack is an attempt to make an online service unavailable by flooding it with traffic from multiple sources. Such an attack is often the result of multiple compromised systems.

8 https://www.welivesecurity.com/2016/11/02/flashback-tuesday-morris-worm

9 https://www.kaspersky.com/blog/morris-worm-turns-25/3065

10 https://www.techopedia.com/definition/5652/us-computer-emergency-readiness-team-us-cert

11 https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

12 https://www.wired.com/2009/07/pci/

13 https://www.wired.com/2010/03/tjx-sentencing/

14 http://large.stanford.edu/courses/2015/ph241/holloway1/

15 https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

16 https://www.reuters.com/article/us-jpmorgan-cybersecurity/jpmorgan-hack-exposed-data-of-83-million-among-biggest-breaches-in-history-idUSKCN0HR23T20141003

17 https://krebsonsecurity.com/tag/jp-morgan-chase-hack/

18 https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

19 https://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html

20 https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?noredirect=on&utm_term=.9eddd1ed82d3

21 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends

22 https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf

23 https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html

24 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends

25 https://www.secureworks.com/resources/rp-2017-state-of-cybercrime

26 https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html

27 https://blog.volkovlaw.com/2018/01/convergence-cybersecurity-compliance-enterprise-risk-management

28 https://www.itgovernance.co.uk/cyber-security-risk-management

29 https://cybersecurityventures.com/cybersecurity-500

30 https://www.fortinet.com/products/utm.html

31 https://www.cbronline.com/enterprise-it/5-unified-threat-management-products-to-simplify-your-cyber-security-4902562

32 https://www.kaspersky.co.in/resource-center/definitions/utm

33 https://digitalguardian.com/blog/what-security-incident-management-cybersecurity-incident-management-process

34 https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/incident_management

35 https://www.business.gov.au/risk-management/cyber-security/prepare-a-cyber-security-incident-response-management-plan

36 https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

37 https://www.g2crowd.com/categories/incident-response-services

38 https://searchsecurity.techtarget.com/definition/identity-access-management-IAM-system

39 https://www.csoonline.com/article/2120384/identity-management/what-is-iam-identity-and-access-management-explained.html

40 https://www.pingidentity.com/en/company/blog/2017/08/14/what_is_identity_and_access_management_iam.html

41 https://cybersecurityventures.com/cybersecurity-500/

42 https://www.paloaltonetworks.com/cyberpedia/what-is-network-security

43 https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider

44 https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider

45 http://www.bladetechinc.com/wp-content/uploads/2015/01/7-layers.pdf

46 https://smallbusiness.chron.com/different-kinds-biometric-security-available-securing-server-room-69885.html

47 https://www.acunetix.com/blog/articles/the-top-5-network-security-vulnerabilities/

48 https://info.focustsi.com/it-services-boston/the-8-layers-of-cybersecurity-needed-to-protect-your-business

49 https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider/

50 https://digitalguardian.com/blog/what-data-encryption

51 https://www.empowerit.com.au/blog/holistic-cybersecurity-7-layers-you-need-to-consider

52 https://www.acronis.com/en-us/articles/data-backup-for-business

53 https://www.unitedlayer.com/sites/default/files/ul-disasterrecoveryguide.pdf

54 https://www.infosecurity-magazine.com/next-gen-infosec/blockchain-cybersecurity

55 https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/acr2018/acr2018final.pdf?dtid=odicdc000016&ccid=cc000160&oid=anrsc005679&ecid=8196&elqTrackId=686210143d34494fa27ff73da9690a5b&elqaid=9452&elqat=2

56 https://www.ibm.com/in-en/security/cognitive?cm_mmc=Search_Google-_-Corporate+Advertising_Pillars-_-AS_IN-_-++ai++cybersecurity&cm_mmca1=000027HR&cm_mmca2=10006695&cm_mmca3=

57 https://www.itgovernance.co.uk/blog/artificial-intelligence-in-cyber-security

58 https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/

59 https://www.techrepublic.com/article/cyberattacks-are-third-largest-threat-to-global-society-over-next-5-years

60 https://eugdpr.org/the-regulation/

61 https://www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know/

62 https://www.insideprivacy.com/united-states/congress-passes-four-cybersecurity-bills

63 https://www.mannheimerswartling.se/globalassets/publikationer/cybersecurity-law-overview.pdf

64 https://www.insideprivacy.com/united-states/congress/congress-passes-the-cybersecurity-act-of-2015

65 https://www.mannheimerswartling.se/globalassets/publikationer/cybersecurity-law-overview.pdf

66 https://www.insidegovernmentcontracts.com/2014/12/fisma-updated-and-modernized

67 https://www.mannheimerswartling.se/globalassets/publikationer/cybersecurity-law-overview.pdf

68 https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

69 https://www.mannheimerswartling.se/globalassets/publikationer/cybersecurity-law-overview.pdf

70 https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

71 https://www.endpointprotector.com/blog/eu-vs-us-how-do-their-data-protection-regulations-square-off

72 http://telecoms.com/492422/us-contemplates-its-own-version-of-gdpr

73 https://www.bloombergquint.com/technology/trump-administration-suggests-tighter-controls-on-consumer-data

74 https://www.reuters.com/article/us-usa-internet-privacy/u-s-seeks-input-on-privacy-rules-to-protect-consumer-data-idUSKCN1M529E

75 https://www.cbsnews.com/news/trump-white-house-data-privacy-proposal-national-telecommunications-information-administration

76 https://www.networkworld.com/article/3286611/data-center/while-no-one-was-looking-california-passed-its-own-gdpr.html

77 https://revisionlegal.com/data-breach/california-data-breach-notification-law

78 https://www.rrmediagroup.com/Features/FeaturesDetails/FID/648

79 https://cybersecurityventures.com/cybersecurity-market-report/

80 https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

81 https://www.marketsandmarkets.com/PressReleases/cyber-security.asp

82 https://www.statista.com/statistics/595182/worldwide-security-as-a-service-market-size/

83 https://in.reuters.com/article/alphabet-chronicle/alphabet-unveils-business-unit-devoted-to-cyber-security-idINKBN1FD2U8

84 https://www.scmagazine.com/home/opinions/blogs/executive-insight/the-debate-is-over-artificial-intelligence-is-the-future-for-cybersecurity/

85 https://chronicle.security

86 https://www.forbes.com/sites/quora/2017/09/14/what-will-cybersecurity-look-like-10-years-from-now/#4939cd9d6e6e

87 https://www.futureofeverything.io/future-of-cybersecurity/

88 https://www.globalsign.com/en-in/blog/cybersecurity-trends-and-challenges-2018

89 https://www.cso.com.au/article/625105/changing-motivations-made-profit-minded-hackers-clear-present-danger

90 https://www.forbes.com/sites/freddiedawson/2015/02/27/could-your-next-start-up-be-in-ethical-hacking/#4cc3654bbb87

91 https://www.ey.com/Publication/vwLUAssets/GISS_report_2017/$FILE/REPORT%20-%20EY%20GISS%20Survey%202017-18.pdf

92 https://techbeacon.com/30-cybersecurity-stats-matter-most

93 http://www.thebull.com.au/premium/a/74644-opportunities-in-cyber-security-stocks.html

94 https://www.bostonhelpdesk.com/obama-investing-19-billion-in-cyber-security-for-2017

95 https://www.janes.com/article/83399/next-year-to-see-sharp-increase-in-french-defence-budget

96 https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html

www.primeindexes.com