**[Challenges and Opportunities of Cyber Security](http://ijsrcseit.com/paper/CSEIT1831486.pdf" \t "_blank)**

Today a man is able to send and receive any form of data may be an e-mail or an audio or a video just with a click of a button without thinking how securely his/her data is being transmitted without any leakage of information. The reason is **Cyber Security**. CyberSecurity is a field of Information Technology involving the protection of computer systems and the prevention of unauthorized use or changes or access of electronic data. It deals with the protection of hardware, software, networks and its information. Cyber security for data networks is in its infancy while the attackers on networks are becoming increasingly sophisticated. Due to the heavy usage of computers in the modern industry that store and transmit a large amount of confidential information about people, cyber security is a critical function and needed insurance of many businesses.

***Novelty of the Innovative Idea-***

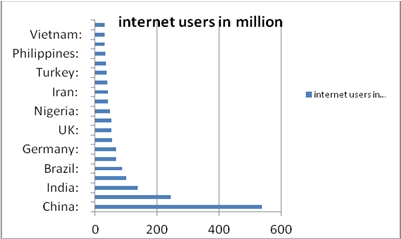
This proposal is the first phase of creating an authenticated routing infrastructure. The work involves adapting advances in evidentiary trust to a link state routing protocol, developing naming for certificate chains and an approach to use the certificates in link state updates. This phase is expected to result in a report and a design for a prototype to be added to open source protocols in a later phase. These results will be made publicly available through open source code and discussions and presentations at standards bodies and with router vendors and network operators. A successful approach should create opportunities to the proposer in contracts with government and commercial organizations. This could result in market opportunities for other organizations such as network management tool and router vendors.

* The arrest of an East German spy in IBM’s German by West Germany’s police in 1968 was acknowledged as the first case of cyber espionage (Warner, 2012, p. 784).
* Ten years ago, “the first real war in cyberspace” attacked Estonia and put the country into “a national security situation” (Hansen and Niessenbaum, 2010, p. 1168).
* The interplay of political expression to the variety of cyber threat (Cavelty, 2013, p. 105) is one of the reasons why it is difficult to approach cyber security issue. Fortunately, this did not stop scholars from trying to discuss the issue.
* Dunn-Cavelty (2010, p. 363) defines Cyber-security as ‘both about the insecurity created through cyberspace and about technical and non-technical practices of making it (more) secure.’ This definition attempt to present that cyber security is not merely a ‘technical’ issue, which always associated with computer science, cryptography or information technology, as with many cyber security related researches that have been discussed in recent years (e.g. Vacca 2013, McLean 2013).**In reality, cyber security entails larger study areas and complex matters.**
* The Dunn-Cavelty’s categorization is based on the interplay between the threats sources and threatened object, and to more understand this relationship, the work of Hansen and Niessanbaum (2010) in using Copenhagen’s securitization theory will be helpful. By using the theory of securitization, they theorize cyber security ‘as a distinct sector with a particular constellation of threats and referent objects’ (Ibid, p. 1155).
* Dewar (2014) explains that ‘the goal of cyber security is to enable operations in cyberspace free from the risk of physical or digital harm’ (p. 18). How country perceive the accumulation of interplays within securitization elements in cyber security issue and the attribution problem makes their cyber security strategy and policy are different each other. Dewar uses triptych term to explain three paradigms of cyber security defense, which are Active Cyber Defense (ACD) that ‘focuses on identifying and neutralizing threats and threat agents both inside and outside the defender’s network, Fortified Cyber Defense (FCD) that ‘builds a protective environment’, and Resilience Cyber Defense (RCD) that ‘focuses on ensuring system continuity’.

# ***Patents –***

## Need for Cyber Security in India

9.4% houses in India have computer (any of Laptop or Desktop). Chandigarh (U/T), Goa and NCT of Delhi are top three stats/union territories with highest computer usage.  
According to 2011 Census, Only 3.1 percent of total houses have [Internet](http://updateox.com/tag/internet/) access in [India](http://updateox.com/category/india/). The census covered 24,66,92,667(246.7 million) houses in India and found only 76,47,473 (3.1%) of this houses use Internet. The Internet includes both [broadband](http://updateox.com/tag/broadband/) and low-speed connections.  
According to Internet World Stats on June 30 2012, there were 2.4 billion internet users (2,405,510,175) worldwide. China was the largest countries in terms of internet users with over 538 million users. The following graph shows top 20 internet countries worldwide at mid-year 2012:



## India’s legal framework for cyber security

* Indian IT Act, 2000

Section 65 - Tampering with computer source code, Section 66 - Hacking & computer offences, Section 43 – Tampering of electronic records

* Indian Copyright Act

States any person who knowingly makes use of an illegal copy of computer program shall be punishable. Computer programs have copy right protection, but no patent protection.

* Indian Penal Code

Section 406 - Punishment for criminal breach of trust and Section 420 - Cheating and dishonestly inducing delivery of property.

* Indian Contract Act, 1872

Offers following remedies in case of breach of contract, Damages and Specific performance of the contract

## ***Concept of this Project-***

## What is Cyber Crime?

Cyber Crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer based variations of existing crimes such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations.

## Why Cyber Crime is more now-a-days?

There are 5 common trends which give chances to Cyber Crime:

* More online transactions and digital data. Transaction and customer information, results of product launches, and other market information are easily available. Creating valuable intellectual property online is an attractive target.
* Comparatively Corporations and companies are expected to be more transparent than before. Majority of people want to access to corporate networks through their mobile devices for day to day activities. Though smarter technology devices increases connectivity and but present latest types of security threats. Hackers can crack these securities and get an easy entry into corporate networks.
* Malicious Software like viruses and spyware are strong enough to take the partial control of main applications.
* In business, customer and vendors are joined to the networks to increase their business profits. In December 2010, a famous E-business website was attacked by dozens of people claiming to be part of the unnamed group. They attempted to perpetrate a denial of service attack in retaliation for website to shut down payment services to other websites. More than a dozen hackers were arrested in that crime.
* There is more technology advanced hackers, professional Cyber Crime organization. For example, hacker receives payment to infect end user device with malware. Today’s Malwares are difficult to trace and they steal data for financial gain. Some people think that they get more money if they become hackers compared to securers.

# ***Methodology for implementation-***

## Methods of attacks

The attacks or methods on the computer infrastructure can be classified into three different categories.

* **Physical Attack**

The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

* **Syntactic Attack**

The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.

* **Semantic Attack**

This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user’s knowledge in order to induce errors.

## Types of Risks

* **Viruses**

This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.

* **Worms**

Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.

* **Trojanhorses**

A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

* **Hacker, attacker, or intruder**

People who exploit weaknesses in software and computer systems for their own gain. Though they do it for curiosity, their actions are typically in violation of the intended use of the systems. The results can range from creating a virus with no intentionally negative impact to stealing or altering information.

* **Malicious code**

This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

* **E-Mail Related Crime**

Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

* **Denial of Service**

These attacks are aimed at denying authorized persons access to a computer or computer network.

* **Cryptology**

Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

# ***Salient features of the project to be implemented-***

## Elements of Cyber Security

* [Application security](http://searchsoftwarequality.techtarget.com/definition/application-security) which is the use of software, hardware, and procedural methods to protect applications from external threats.
* Information security is the practice of avoiding [information](http://en.wikipedia.org/wiki/Information) from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. IT Security and Information assurance are two major aspects of information security.
* Network security which consists of the provisions and [policies](http://en.wikipedia.org/wiki/Policies) adopted by a [networkadministrator](http://en.wikipedia.org/wiki/Network_administrator). They prevent and monitor [unauthorized](http://en.wikipedia.org/wiki/Unauthorized) access, misuse, modification, or denial of a [computer network](http://en.wikipedia.org/wiki/Computer_network) and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.
* [Disaster recovery](http://searchenterprisewan.techtarget.com/definition/disaster-recovery-plan) / [business continuity planning](http://searchdisasterrecovery.techtarget.com/definition/business-continuity-action-plan) - need to encompass [how employees will communicate, where they will go and how they will keep doing their jobs](http://www.csoonline.com/article/220446). The details can vary greatly, depending on the size and scope of a company and the way it does business. For some businesses, issues such as [supply chain logistics](http://www.csoonline.com/topic/41252/Supply_Chain) are most crucial and are the focus on the plan. For others, information technology may play a more pivotal role, and the BC/DR plan may have more of a focus on systems recovery. For example, the plan at one global manufacturing company would restore critical mainframes with vital data at a backup site within four to six days of a disruptive event, obtain a mobile PBX unit with 3,000 telephones within two days, recover the company's 1,000-plus LANs in order of business need, and set up a temporary call center for 100 agents at a nearby training facility.
* End-user education involves educating end users with various information attacks and how to avoid them. For example, while registering password, tell end user what should be the length and characteristics of complex password. Provide suitable education about what are the precautions they have to take to avoid Cyber Crimes. Also, sometimes actions to be taken in case if they are victim.

## Challenges is Cyber Security

Cyber security has been considered as one of the most urgent [national security](http://itlaw.wikia.com/wiki/National_security) problems. A report says, in a speech during his presidential campaign, President Obama promised to “make cyber security the top priority that it should be in the 21st century and appoint a National Cyber Advisor who will report directly” to the President.

Cyber security must address not only deliberate [attacks](http://itlaw.wikia.com/wiki/Attack), such as from disgruntled employees, [industrial espionage](http://itlaw.wikia.com/wiki/Industrial_espionage), and [terrorists](http://itlaw.wikia.com/wiki/Terrorist), but inadvertent [compromises](http://itlaw.wikia.com/wiki/Compromise) of the [information infrastructure](http://itlaw.wikia.com/wiki/Information_infrastructure) due to [user errors](http://itlaw.wikia.com/wiki/User_error), equipment failures, and natural disasters. [Vulnerabilities](http://itlaw.wikia.com/wiki/Vulnerabilities) might allow an [attacker](http://itlaw.wikia.com/wiki/Attacker) to [penetrate](http://itlaw.wikia.com/wiki/Penetrate) a [network](http://itlaw.wikia.com/wiki/Network), gain [access](http://itlaw.wikia.com/wiki/Access) to [control software](http://itlaw.wikia.com/wiki/Control_software?action=edit&redlink=1), and alter [load conditions](http://itlaw.wikia.com/wiki/Load_condition?action=edit&redlink=1) to destabilize a [network](http://itlaw.wikia.com/wiki/Network) in unpredictable ways.

The defense of cyberspace necessarily involves the forging of effective partnerships between the public organizations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The defense of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

## Other Indian Government Initiatives

Indian government released National Cyber Security Policy on July 2, 2013. This policy addressing the growth of information technology, increasing number of Cyber Crimes, plans for social transformation [6]. It has 14 objectives which includes enhancing the protection of India’s Critical infrastructure to investigation and prosecution of Cyber Crime, developing 50,000 skilled cyber security professionals in next five years.

* Cyber Security Research And Development Centre Of India (CSRDCI) -This concentrates on Techno Legal Cyber Security Issues of India and World Wide. This Platform and Website is managed by [Perry4Law](http://www.perry4law.com/), [Perry4Law Techno Legal Base (PTLB)](http://www.ptlb.in/) and [Perry4Law Techno Legal ICT Training Centre (PTLITC)](http://ptlb.co.in/).The Cyber Security Initiatives and Projects of PTLB at a single place.
* Cyber Crimes Investigation Centre Of India -The [Cyber Crime Investigation Centre of India (CCICI)](http://ptlb.in/ccici/) is the exclusive [Techno Legal Cyber and Hi-Tech Crimes Investigation and Training Centre (CHCIT) of India](http://perry4law.co.in/cc.html). The objective of CCICI is to spread [Cyber Law Awareness](http://perry4law.org/cecsrdi/?p=830) and [Cyber Security Awareness in India](http://perry4law.org/cecsrdi/?p=748) and abroad. Further, CCICI also intends to develop [Cyber Crimes Investigation Capabilities and Expertise in India](http://ptlb.in/ccici/?p=12) and abroad.
* National Intelligence Grid (NATGRID) - This Project of India is one of the most ambitious Intelligence Gathering Project of India. It has been launched at a time when the [Intelligence Infrastructure of India](http://ptlbindia.blogspot.com/2011/03/intelligence-infrastructure-of-india-is.html) is in a bad shape. It is an essential requirement for robust and effective Intelligence Agencies and Law Enforcement functions in India.
* National Critical Information Infrastructure Protection Centre (NCIPC) Of India - intends to ensure critical infrastructure protection and critical ICT infrastructure protection in India.
* [National Cyber Security Database of India (NCSDI)](http://perry4law.co.in/cyber_security/?p=23) - This Database would work in the direction of fighting against Cyber Threats and Cyber Attacks including [Cyber Terrorism Against India](http://www.ptlb.in/blog/?p=193), [Cyber Warfare Against India](http://www.ptlb.in/blog/?p=221), [Cyber Espionage Against India](http://www.ptlb.in/blog/?p=151), [Critical Infrastructure Protection in India](http://www.ptlb.in/blog/?p=243), [Managing India’s Cyber Security Problems, Issues and Challenges](http://perry4law.co.in/cyber_security/?p=65), etc.

## Indian Government Initiatives for Education on Cyber Security

* Information security awareness – This is launched from over a five years period. One of the objectives is to create awareness about information security to children, home users and non-IT professionals in a systematic way. C-DAC Hyderabad has been assigned this project.
* Information security education and awareness project- Objectives are to train System Administrators by offering Diploma Course in Information Security, Certificate Course in Information Security, 6-weeks/2-weeks training programme in Information Security, train Government Officers of Center and State on Information Security issues and Education Exchange Programme
* National Initiative for Cyber Security Education (NICE) - The goal of NICE is to establish an operational, sustainable and continually improving cyber security education program for the nation to use sound cyber practices that will enhance the nation’s security.

# ***Objectives –***

The cyber security objectives set by countries, as defined in their NCSS (National Cyber Security Strategies), all adopt a very similar pattern and can broadly be grouped as follows:

* To guarantee citizens' operations in cyberspace
* To protect government ICT infrastructures
* To protect the ICT aspect of critical infrastructures
* To improve cyber security professionals' skills and citizen sensitization and awareness
* To encourage public-private partnerships
* To boost international cooperation

In short, the goal is to guarantee the security of citizens' online operations by protecting key infrastructures involved in the provision of these services.

In the case of the Spanish National Cyber Security Strategy, the overall goal is the secure use of ICT infrastructures. Prevention, defense and the response to cyber attacks. The specific objectives are as follows:

* To guarantee a level of cyber security for government ICTs
* To promote security and resilience in the business sector and among IC operators
* To reinforce prevention, detection, reaction, analysis, recovery, response and research skills to cope with terrorism and cyber delinquency
* To sensitize citizens and the public and private sectors to the risks derived from cyber space.
* To obtain and maintain technological knowledge, experience and skills in Spain in order to support the cyber security objectives
* To play a role in improving cyber security in the international arena

As we can see, all very much in line with the other NCSS we've published. From the point of view of an internationally focused company like Indra, the private sector can play a very powerful role in helping to fulfill these objectives, especially as regards the provision of cyber security services, training, skills, sensitization and international collaboration.

# ***Budget for implementation of research & development projects in the identified areas of innovation-***

This recommended list is based upon a classroom size of 25 students. All costs are estimated and should be adjusted and verified with current quotes. No specific equipment vendor or brand names are listed due to various possibilities. The intent of this list is to provide school districts with guidance on the necessary equipment needs to cover the state standards for a Cybersecurity program.

Classroom equipment Total: 1059100/-

|  |  |  |  |
| --- | --- | --- | --- |
| QTY | ITEM DESCRIPTION | UNIT | TOTAL |
| 25 | Student Workstations w/chairs | 28000/- | 700000/- |
| 1 | Teacher Workstation w/chair | 28000/- | 28000/- |
| 1 | Teacher Computer | 63000/- | 63000/- |
| 1 | Classroom Smartboard | 140000/- | 140000/- |
| 1 | Networkable Laser Printer | 28000/- | 28000/- |
| 1 | LCD Projector | 56000/- | 56000/- |
| 1 | Storage Cabinet (36” x 12” x 72”) (lockable) | 21000/- | 21000/- |
| 1 | Vertical File Cabinet (4 drawer, lockable) | 23100/- | 23100/- |

Program equipment Total: 4438000/-

|  |  |  |  |
| --- | --- | --- | --- |
| QTY | ITEM DESCRIPTION | UNIT | TOTAL |
| 25 | Student Laptop Computers | 70000/- | 1750000/- |
| 15 | Cisco 2901 ISR Router | 127400/- | 1911000/- |
| 6 | Rack mount Patch Panels w/12 ports | 42000/- | 252000/- |
| 15 | PC Assembly Kits | 38500/- | 525000/- |

Instructional materials Total: 185500/-

|  |  |  |  |
| --- | --- | --- | --- |
| QTY | ITEM DESCRIPTION | UNIT | TOTAL |
| 25 | Student Textbooks (Approved by NDE) | 7000/- | 175000/- |
| 1 | Teacher Textbook Edition and References | 10500/- | 10500/- |

Instructional supplies Total: 1001560/-

|  |  |  |  |
| --- | --- | --- | --- |
| QTY | ITEM DESCRIPTION | UNIT | TOTAL |
| 1 | IOS Tablet | 31500/- | 31500/- |
| 1 | Android Tablet | 31500/- | 31500/- |
| 1 | Bulk UTP Cable, CAT 6 (1000 ft roll) | 28000/- | 28000/- |
| 5 | Networking Rack-Open Frame (free standing to hold 6 devices) | 28000/- | 140000/- |
| 15 | Cisco 8-10 Port Switch (rack mountable) | 10500/- | 157500/- |
| 1 | Bulk UTP Cable, CAT 5e (1000 ft roll) | 9100/- | 9100/- |
| 15 | Anti-static Screen Wipes | 8400/- | 126000/- |
| 15 | Network Software Anti-Virus | 7000/- | 105000/- |
| 1 | Wireless Access Point / Network | 7000/- | 7000/- |
| 5 | Digital Multimeter Tester | 5950/- | 29750/- |
| 15 | Network Technician Toolkit (to include 3-in-1 crimping tool, UTP/STP wire stripper and cutter, punchdown tool, LAN cable tester, tone and probe) | 5600/- | 84000/- |
| 5 | Electric Blower/ Duster | 5250/- | 26250/- |
| 15 | VGA Cables (various lengths/endings) | 5250/- | 78750/- |
| 15 | PC Technician Toolkit | 3500/- | 52500/- |
| 15 | Mounting Brackets | 1400/- | 21000/- |
| 30 | Anti-Static Work Mats | 1050/- | 31500/- |
| 30 | Anti-Static Wristbands | 1050/- | 31500/- |
| 40 | Safety Goggles | 210/- | 8400/- |
| 5 | RJ45 Connectors (box of 100) | 210/- | 1050/- |
| 5 | RJ45 Punchdown Keystone Jack - Dual Row (box of 100) | 210/- | 1050/- |
| 1 | RJ45 Inline Couplers (box of 60) | 210/- | 210/- |

# ***Why Cyber Security is essential for Engineering students –***

# *Ethical Reasons-*

## **The rising cost of breaches**

The fact is that cyber attacks can be extremely expensive for businesses to endure. Recent statistics have suggested that the average cost of a data breach at a larger firm is £20,000. But this actually underestimates the real expense of an attack against a company. It is not just the financial damage suffered by the business or the cost of remediation; a data breach can also inflict untold reputational damage.

Suffering a cyberattack can cause customers to lose trust in a business and spend their money elsewhere. Additionally, having a reputation for poor security can also lead to a failure to win new contracts.

## **Increasingly sophisticated hackers**

Almost every business has a website and externally exposed systems that could provide criminals with entry points into internal networks. Hackers have a lot to gain from successful data breaches, and there are countless examples of well-funded and coordinated cyber-attacks against some of the largest companies in the UK. Ironically, even [Deloitte](https://www.consultancy.uk/firms/deloitte), the globe’s [largest cybersecurity consultant](https://www.consultancy.uk/news/13927/the-worlds-top-10-largest-cybersecurity-security-consulting-firms), was itself [rocked by an attack](https://www.consultancy.uk/news/14068/largest-cybersecurity-consultant-of-the-world-rocked-by-cyber-attack) in October last year.

With highly sophisticated attacks now commonplace, businesses need to assume that [they will be breached](https://www.redscan.com/news/mssp-mdr-evolving-managed-security-market/) at some point and implement controls that help them to detect and respond to malicious activity before it causes damage and disruption.

## **Widely available hacking tools**

While well-funded and highly skilled hackers pose a significant risk to your business, the wide availability of hacking tools and programmes on the internet also means there is also a growing threat from less skilled individuals. The commercialisation of cybercrime has made it easy for anyone to obtain the resources they need to launch damaging attacks, such as ransomware and cryptomining.

## A proliferation of IoT devices

More smart devices than ever are connected to the internet. These are known as Internet of Things, or IoT, devices and are increasingly common in homes and offices. On the surface, these devices can simplify and speed up tasks, as well as offer greater levels of control and accessibility. There proliferation, however, presents a problem.

If not managed properly, each IoT device that is connected to the internet could provide cyber criminals with a way into a business. IT services giant Cisco estimates there will be 27.1 billion connected devices globally by 2021 – so this problem will only worsen with time. With use of IoT devices potentially introducing a wide range of security weaknesses, it is wise to conduct regular vulnerability assessments to help identify and address risks presented by these assets.

## Tighter regulations

It is not just criminal attacks that mean businesses need to be more invested in cyber security than ever before. The introduction of [regulations such as the GDPR](https://www.consultancy.uk/news/15795/gdpr-spurs-companies-to-boost-cybersecurity-precautions) means that organizations need to take security more seriously than ever, or face heavy fines.

The GDPR has been introduced by the EU to force organizations into to taking better care of the personal data they hold. Among the requirements of the GDPR is the need for organizations to implement appropriate technical and organizational measures to protect personal data, regularly review controls, plus detect, investigate and report breaches.

# *Professional Reasons-*

## **Your services will be in great demand.**

Given omnipresent reports about cyber crime, it’s hardly a surprise that experts are predicting a worldwide shortage of information security professionals looking toward the future. [Symantec CEO Michael Brown told CSO Online’sCybersecurity Business Report](http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html), “The demand for the (cybersecurity) workforce is expected to rise to 6 million (globally) by 2019, with a projected shortfall of 1.5 million.”

It’s hardly a surprise that Infosecurity routinely tops lists of the best jobs out there. It was recently [ranked eighth](https://money.usnews.com/careers/best-jobs/information-security-analyst) on U.S. News and World Report’s rankings of top careers, due in no small part to a meteoric growth rate of 36.5 percent over the next half-decade.

## **Your work will have purpose.**

Job security is indeed a plus, but it’s far from the only thing. IBM CEO GinniRometty once declared cyber crime to be “[the greatest threat to every company in the world](https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#461af2b973f0).”  The takeaway? If you’re looking to make a difference in your career, cybersecurity offers the chance to save and protect sensitive, personal information from hackers and cyber attacks.

And while you may not become famous for your efforts, you’ll still be providing an essential and noble service. [Says SecurityIntelligence.com](https://securityintelligence.com/six-reasons-why-every-student-should-consider-a-career-in-cybersecurity/), “What’s under constant attack is more than just our networks, devices, servers, applications and data; it’s also our mobile, flexible, connected way of life. Very much like the thin blue line of law enforcement or the thin red line of firefighters, the thin digital line of cybersecurity professionals will increasingly be recognized and appreciated as an important and meaningful vocation.”

## **The financial incentives are many.**

While the chance to serve the greater good is a compelling one, doing so won’t pay your bills. The good news? Cybersecurity professionals are extremely well compensated for their skills and talents. In fact, [according to recent figures from DICE](http://media.dice.com/report/may-2015-top-paying-tech-security-jobs/), information security professionals, including lead software security engineers, directors of security, and security consultants, can all can expect to make upwards of $200,000 salaries -- more than CSOs!

Not only that, but salaries rise with demand, so as the shortage increases so will your earning potential.

## **You can work in many different industries.**

While technology-related fields may come to mind when you hear the word “cybersecurity,” the reality is that in today’s digital landscape, all industries -- from banks and finance to education and nonprofits -- require information security services.

While demand will be universal for analysts with innovative minds and the skills to back them up, two areas in particular are expected to experience meteoric growth. Says the [Bureau of Labor Statistics](https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6), “The federal government is expected to greatly increase its use of information security analysts to protect the nation’s critical information technology (IT) systems. In addition, as the healthcare industry expands its use of electronic medical records, ensuring patients’ privacy and protecting personal data are becoming more important. More information security analysts are likely to be needed to create the safeguards that will satisfy patients’ concerns.”

## **You’ll get to call the shots.**

One last thing to keep in mind about cybersecurity? Because of its unique combination of in-demand status and inherently digital nature, cybersecurity professionals have a lot of bargaining power when it comes to finding work.

Reveals CSO Online, “Cybersecurity pros are most likely to leave to find more challenging work, better pay, and more flexible working hours, according to a survey released this morning. Office location also played an unexpected role in employees' decision as well.”  As a result, companies looking to hire (and retain) the best people, are charged with coming up with “more meaning, flexibility and growth opportunities,” including everything from more exciting work to more flexible working conditions. On the receiving end of these upsides? Sought-after cybersecurity professionals.

If you’re sold on a career in cybersecurity but not sure a return to campus life is for you, you’re not out of luck. Many universities offer extensive online programming, courses and degree programs aimed at helping prepare the next generation of cybersecurity experts with the knowledge, skills and experience they need to succeed in this dynamic field.The best part? You don’t even have to [wear a cape](https://video.search.yahoo.com/search/video?fr=mcafee&p=cape+incredibles+youtube#id=3&vid=f694d15df5c318adcc54603025e5ed81&action=click) to be a (cyber) security hero.

# ***Reference-***

1. Dewar, R. 2014. ‘the Triptych of Cyber Security: A Classification of Active Cyber Defense’. 6th International Conference on Cyber Security
2. Dunn-Cavelty, M. 2010. ‘Cyber Security’ in A. Collins, Contemporary Security Studies. Oxford: OUP
3. Dunn-Cavelty, M. 2013. From Cyber-Bombs to Political fallout: threat Representations with an impact in Cyber-Security Discourse. International Studies Review, 15, pp. 105-122
4. Hansen, L. and Niessanbaum, H. 2009. Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, pp. 1155-1175
5. McLean, S. 2013. Beware the Botnets: Cyber Security is a Board Level Issue.Intellectual Property & Technology Law Journal, 25 (12), pp. 22-27
6. Warner, M. 2012. Cybersecurity: A Pre-history. Intelligence and National Security, 27 (5), pp. 781-799
7. Vacca, JR. 2013. Cyber Security and IT infrastructure protection. Waltham: Steven Elliot