The Talent Crisis in InfoSec

An Outlook of the Future of the Indian Information Security Scenario by EC-Council Foundation
Introduction

The arrival and acceptance of the internet as a part of our daily life has changed our lives dramatically. It has enabled easy flow of information that has proved to be both a boon and a bane. Geographical boundaries are no longer a hurdle in accessing information and this has opened the market for knowledge sharing not just with friends and acquaintances but also strangers. This connected world, however, brings threats of being compromised and falling prey to cyber criminals. These criminals use techniques like data tampering, buffer overflow, cross-site scripting, SQL injection, denial-of-service attacks and many more to attain their goal – compromising vulnerable systems.

Today, we take measures to protect our critical data online- bank accounts details, social security details, family details and most importantly our personal details. A single assault on our virtual data can lead to not just a compromise of our reputation but could also have fatal consequences. For instance, there have been instances where insulin pumps sold by a medical equipment manufacturers were vulnerable to wireless hacking. This resulted in an attacker remotely disabling the pumps or manipulating certain settings, like the insulin dosage that is automatically delivered to the patient.

The key question remains. Why are these attacks so prevalent? Why is the cyber security community’s effort is not yielding results that are affecting a positive change? In this report, we hope to bring to light some key factors, that, based on our research, has undeniably contributed to the global phenomenon of “cyber insecurity”.

We hope that we will be able to draw the attention to the importance of developing critical skills that are required in the (InfoSec) industry today for India to sustain its leadership as the software hub for the world.

These were the questions that prompted EC-Council Foundation to commission a research project in India to measure the sensitization of software engineers towards InfoSec risks that we face today. In this report, we hope to bring to light some key factors, that, has undeniably contributed to the global phenomenon of “cyber insecurity”.

Jay Bavisi,
Chairman, EC-Council Foundation
# Table of Contents

Key Highlights ................................................................................................................. 03

Executive Summary .......................................................................................................... 03

Methodology ...................................................................................................................... 04

Code Uncode ..................................................................................................................... 05

Talent Requirement and Shortage of Skills ........................................................................ 06
  - What is information security? ....................................................................................... 06
  - Which sectors is IT required in? .................................................................................. 07
  - What are the profiles and skills where information security is required? ........ 08-09

The Talent Crisis ............................................................................................................... 10
  - All India Analysis ...................................................................................................... 10-11
  - The North ................................................................................................................. 12
  - The East .................................................................................................................... 13
  - The West ................................................................................................................... 14
  - The South .................................................................................................................. 15

Dangers of Lack of Talent .................................................................................................. 16

Conclusion ......................................................................................................................... 17

Appendix ............................................................................................................................ 18-19

End Notes .......................................................................................................................... 19

Supporting Colleges ......................................................................................................... 20-21

About EC-Council Foundation .......................................................................................... 22

Contact Us ......................................................................................................................... 23
Key Highlights

• India’s talent pipeline in information security skills is weak with just under a percentage of student population in engineering equipped with basic skills in information security.

• Among the North, West, East, South – East and North shows a more promising set of skills in information security.

• An evaluation also underscores that basic training in information security should be mandatory, as the requirement of professionals spans across sectors including IT, ITeS, Financial, Government in fact any large organization has requirement of information security technicians.

Executive Summary

Gottfried Leibniz, who discovered Binary in 17th century, would never have envisioned the role that binary would play in the 21st century, that, a massive ecosystem involving governments, businesses, academia and individuals would stand on the numeral system. As one of the largest trainers worldwide in InfoSec, EC-Council Foundation, in its capacity is involved in making this system more secure and enforcing more security in the digital twin world that we all live in today.

This report is a step towards understanding our education system and in making the cyber world more secure. The vulnerability lies in envisioning the talent required in the field in the near future. By 2015, India needs at least 500,000 cyber professionals. Yet, only under a percent of future IT professionals seem to be well trained in InfoSec.

The report has identified that a larger chunk of talent has little understanding of even basic skills.

• Only 0.97% of students in India have the basic skills in Information Security.

• Only about a 13% of students have an understanding of concepts and can be trained in information security.

• More than 86% have not been made aware of skills or are not Trainable by companies on the subject.

This represents a very bleak scenario, impacting the very future of India – government, businesses and individuals. The report urges the nation to take corrective steps in building a workforce with trained talent.
Methodology

The analysis for the report is based on a sample size of more than 10,000 students from various academic institutions. All these students appeared for a nationwide competition, Code Uncode, held by EC-Council Foundation for students, to assess their knowledge in information security.

The sample size was classified into four zones, namely, East, West, North and South. The participants hailed from IT and Engineering colleges across India.

Using their test scores and applying statistical tools on these scores, participants were classified into three groups, which were: Ineligible, Skilled, and Trainable talent.

- **Skilled talent** is a group of participants with ample understanding of basics of InfoSec and are ready to enter the industry. We classified this group by calculating test scores that were more than the average scores + 3x Std. Deviation.

- **Trainable talent** is a group of participants with low understanding of InfoSec, but are equipped with programming skills and have clarity on basic terms of InfoSec, and are trainable by any company that hires them. We classified this group by calculating test scores that were more than the average scores +1x Std. Deviation but less than average scores + 3x Std. Deviation.

- **Ineligible talent** is a group of participants who are unequipped with even the basic skills on InfoSec and have a low understanding of programming languages. We classified this group by calculating test scores that were less than the average scores + 1x Std. Deviation.

### Breakup of States where participants hailed from

<table>
<thead>
<tr>
<th>NORTH</th>
<th>SOUTH</th>
<th>EAST</th>
<th>WEST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jammu &amp; Kashmir</td>
<td>Andhra Pradesh</td>
<td>Chhattisgarh</td>
<td>Maharashtra</td>
</tr>
<tr>
<td>Jharkhand</td>
<td>Tamil Nadu</td>
<td>West Bengal</td>
<td>Gujarat</td>
</tr>
<tr>
<td>Himachal Pradesh</td>
<td>Karnataka</td>
<td>Meghalaya</td>
<td>Goa</td>
</tr>
<tr>
<td>Uttar Pradesh</td>
<td>Kerala</td>
<td>Tripura</td>
<td></td>
</tr>
<tr>
<td>Haryana</td>
<td></td>
<td>Assam</td>
<td></td>
</tr>
<tr>
<td>Delhi</td>
<td></td>
<td>Orissa</td>
<td></td>
</tr>
<tr>
<td>Madhya Pradesh</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rajasthan</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Code Uncode - India’s First Ever Secure Programming Competition

Code Uncode was an initiative by EC-Council Foundation to search for the top secure programmers in India. Happening for the first time in India, the aim of Code Uncode was to spur the growth in information security.

This was a nationwide event where we invited colleges and corporates to participate and compete on the various levels of the competition. The event brought together over 10,000 candidates from over 100+ colleges to compete against each other, assess their secure coding skills and aim to win the title of India’s most secure programmer.

The aim of Code Uncode was to build capacity - to inspire development of InfoSec professionals of the future and to build awareness - to spur growth in educations and ethics in InfoSec.

The analysis conducted in this report has been done purely on the basis of the data and results collected from the 100+ colleges across India that participated in Code Uncode and are representative of India’s future IT workforce. The competition also helped decipher the current level of training that the participants have received.

Together with the scores of Code-Uncode, India’s first nation-wide secure programming competition initiated by EC-Council Foundation, the above analysis was drawn. Various demographic details of the candidates were captured by the testing platform, to arrive at the quality of the talent pool in the information security domain.
What is information security?

Information security, sometimes abbreviated as InfoSec, is the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a generic term that can be used regardless of the form the data might take (electronic, physical, etc...).

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and finances. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about business customers or finances or new product lines fall into the hands of a competitor or a black hat hacker, it could lead to exploited data and/or information, exploited staff/personnel, fraud, theft, and information leaks. Also, irreparable data loss and system instability can result from malicious access to confidential data and systems. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.
**Which sectors is IT required in?**

India requires over 5 lakh Information Security professionals in the upcoming years, a statement repeatedly quoted in the media over the past few months. The depth of the requirement is immense and critical while the supply is inadequate. Information Security is such a diverse domain that a trained professional in this field can find placement in multiple roles, namely, as a network security systems manager, network security administrator, network security engineer, web security administrator, web security auditor, application security tester, ethical hacker, information security analyst, database and software developer, data security specialist, and chief information security officer to name a few.

Almost every big organization generates a large requirement for Information security professionals, however, Govt, IT/ITes, Financial institutions, Telecom, Mobility, Internet organizations and Hospitals worldwide are more vulnerable to cyber threats today because of the data they handle and for the security of this, need skilled professionals.

In a recent move to up the ante on cyber security, the government hired 4446 experts. But the important question here is, is it an inadequate number in a very exposed system? Similarly the corporate world in India has just started to acknowledge the need and the dearth of professionals in the field, with leading corporates taking steps in the direction.

**A Comparative Study**

**US CYBER SECURITY PLAN**

- Courses in Universities and Colleges (DHS, EBK, NICE, DoD 8570, CISSE, CNSS)
- Training and Labs (DHS, EBK, NICE, DoD 8570, CISSE, CNSS)
- Programs
- Incentives
- 15 Percent more Cyber Security Experts Every Year

**INDIA’S CYBER SECURITY PLAN**

- Courses in Universities and Colleges (DHS, EBK, NICE, DoD 8570, CISSE, CNSS)
- Training and Labs
- Programs
- Incentives
- 5 Lakh Cyber Security Experts
Opportunities in InfoSec

What are the profiles and skills where information security is required?

1. **Security Analyst**
   - Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information
   - Ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure
   - Respond to computer security breaches and viruses

2. **Security Auditor**
   - Security auditors work with a company to provide an audit of security systems used by that company
   - Once completed, the security auditor will provide the company with a detailed report of information systems. These reports will outline whether the system runs efficiently or effectively. This can help the company make changes where necessary to improve the integrity of their system
   - Oversees, evaluates, and supports the documentation, validation, and accreditation processes necessary to assure that new IT systems meet the organization's IA requirements
   - Ensures compliance from internal and external perspectives

3. **Analyst Programmer**
   - Computer programmers write code to create software programs
   - They turn the program designs created by software developers and engineers into instructions that a computer can follow
   - Troubleshoot network operation issues and facilitate smooth information flow
   - Monitor and analyze network performance across the organization’s LANs, WANs and wireless deployments
   - Focus upon network components within a company’s LAN/WAN infrastructure ensuring security and integrity of information systems

4. **Network Administrator**
   - Design and deploy networks based on the business requirement
   - Help organizations procure network hardware and software
   - Implement and manage network and routing protocols, implement of authentication and authorization controls
   - Responsible for maintaining disk images and backups
   - Install and configure all network hardware and equipment, including routers, switches, hubs, UPS, etc.

5. **Information security professional**
   - Ensures networks, infrastructure, and computer systems within organizations are properly and adequately secure by protecting information assets, such as customer data, financial information and critical network infrastructures
   - Performs security threat and risk analysis
   - Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.
   - Lead the development/adoption and enforcement of Information Security policies, procedures and standards

6. **Project Manager**
   - Develops and implement the project plan
   - Manages the team's performance of project tasks
   - Secures acceptance and approval of deliverables from the Project Sponsor and Stakeholders
   - Holds responsibility for communication, including status reporting, risk management, escalation of issues that cannot be resolved in the team
   - Ensures the project is delivered on budget, on schedule, and within scope
The Talent Crisis

All India analysis

A cursory understanding of the talent situation in India provides a very gloomy picture. Since just one percent of students in India are equipped with skills pertaining to information security, this would eventually result in weakening of business in certain sectors, or become a point of contention in upholding a sector.

As shown in Figure 1 below,

- Only 1% of students in India have the basic skills in Information Security.
- Only about a 13% of students have an understanding of concepts and can be trained in information security.
- More than 86% have not been made aware of skills or are Trainable in the subject.

Snapshot of National level talent

% break-down of Skilled, Trainable, and Ineligible talent in India

EC-Council Foundation Analysis

All India performance of talent

Trend line chart representing scores of participants, indexed to 100
A closer analysis gives us an idea of how the potential information security personnel are trained in the country. Figure 2 above reflects the volume of students within a certain range. The peak indicating the maximum students is closer to 28 which is the average score of participants across India, and the range of scores is from 20 to 40, affirming that discovery of the subject has happened. We hypothesize that course curriculum has inbuilt topics on InfoSec; however, it is not a separate subject and is not studied in great detail. A smaller crest is visible at the end, which represents a chunk of trained talent indicating a set of students who are getting adequate training in information security.
The North

- Although very low in terms of absolute data, a relatively higher percentage of students from North India are Skilled in information security.
- About an 18% of students are Trainable in the region.
- It emerges that talent in tier 2 cities within the region is also Trainable.
- Cities that have good talent include Varanasi, Bareilly and Noida among others.

Snapshot of talent in the North

% break-down of Skilled, Trainable, and Ineligible talent in the North

EC-Council Foundation Analysis

Performance of talent in the North

Trend line chart representing scores of participants, indexed to 100.

The distribution of talent is not as low as the all-India mark, and we see a bulk of talent in the 30-50 range.
The East

- Scoring highest on the percentage of Trainable talent, it comes as a surprise that the East has almost 20% of students with some understanding of information security.

- About 1.5% of students are equipped with information security skills, while 79% are not Trainable at all.

- Cities in the region with a good talent pool include Gangtok and Kolkata among others.

Snapshot of talent in the East

% break-down of Skilled, Trainable, and Ineligible talent in the East

![EC-Council Foundation Analysis](image)

Performance of talent in the East

Trend line chart representing scores of participants, indexed to 100

![Score Distribution](image)

The peak in the trend line is an indicator of a higher degree of trained talent in the region.
The West

- Contributing a chunk of engineering talent to the country, this region lags behind in trained talent, with just under 10% of Trainable talent. Discouragingly, less than 0.2% of the talent is trained.

- Cities in the region with a good talent pool include Nagpur and Ahmedabad among others.

**Snapshot of talent in the West**

% break-down of Skilled, Trainable, and Ineligible talent in the West

![Pie chart showing the percentage breakdown of skilled, trainable, and ineligible talent in the West. Skilled: 0.2%, Trainable: 9.7%, Ineligible: 90.1%]

**Performance of talent in the West**

Trend line chart representing scores of participants, Indexed to 100

![Trend line chart showing the distribution of scores with a notable drop in the range 50-60, indicating a very low percentage of Trainable talent.]

The range of the bulk of talent here moves to 25-40, emphasizing on a greater need for even basic understanding of concepts. There is a considerable drop in the trend line at range 50-60 indicating a very low percentage of Trainable talent.
The South

- A most important region for sourcing talent within the country, South again seems to have very a small percentage of trained talent and Trainable talent when compared to the rest of the country. This is alarming as most of the talent in IT industry is sourced from this region. Cognizance of information security skills lacks the most in this part of the country.

- Cities with Trainable talent in the region include Hyderabad, Comibatore, Chennai and Bangalore.

**Snapshot of talent in the South**

% break-down of Skilled, Trainable, and Ineligible talent in the South

[Diagram showing percentage distribution]

**Performance of talent in the South**

Trend line chart representing scores of participants, indexed to 100

[Graph showing score distribution]

In what is a very peculiar case, South shows low promise on trained talent and low scope on Trainable talent. This may be attributed to the fact that South has high number of colleges and most of them do not proactively focus on information security as a subject.
Dangers of Lack of Talent

<table>
<thead>
<tr>
<th>Category</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poor Input and Data Validation</td>
<td>- Buffer overflow&lt;br&gt;- Cross-site scripting&lt;br&gt;- SQL injection</td>
</tr>
<tr>
<td>Poor Authentication and Authorization Mechanism</td>
<td>- Credential theft&lt;br&gt;- Eavesdropping&lt;br&gt;- Privilege escalation</td>
</tr>
<tr>
<td>Insecure Data Storage</td>
<td>- Accessing sensitive data in storage and memory</td>
</tr>
<tr>
<td>Poor Session Management</td>
<td>- Session hijacking</td>
</tr>
<tr>
<td>Insecure Exception and Error Handling</td>
<td>- Disclosure of sensitive information</td>
</tr>
<tr>
<td>Poor Configuration Management</td>
<td>- Illegal access to administration interfaces</td>
</tr>
<tr>
<td>Weak Cryptography</td>
<td>- Loss of decryption keys</td>
</tr>
<tr>
<td>Improper Auditing and Logging</td>
<td>- Denial of performing an operation by user</td>
</tr>
<tr>
<td>Improper File Handling</td>
<td>- Malicious file inclusion</td>
</tr>
</tbody>
</table>

To quote some real life instances, **distributed denial of service attacks** have been used to divert security personnel attention while millions of dollars were stolen from banks, according to industry data. Well known US banks have been plundered by fraudulent wire transfers while hackers deployed “low powered” DDoS attacks to mask their theft and have brought down web sites belonging to JP Morgan, Wells Fargo, Bank of America, Chase, Citigroup, HSBC, and others.

Sensitive information has been disclosed and misused on multiple occasions due to **insecure data storage** and the **Man-in-the-Middle(MITM)** attack is a recurring nuisance due to due to poor implementation of authentication and authorization mechanism.

Similarly, **unvalidated redirect/ website defacement** attacks due to **poor input validation** have also had serious repercussions like the time the Syrian Electronics Army attacked the marines website saying ‘Obama is a Traitor’.
Conclusion

We believe that to achieve success in any field it is imperative to not only identify the gaps and have a clear vision of the future, but also to chalk out steps to reach those goals we foresee. Industry data and reports have shown time and again that there is a large demand for skilled InfoSec professionals in the industry today. The research above, along with a detailed study by EC- Council Foundation has proved that our current talent pool is not even remotely close to meeting that demand. Low awareness and lack of initiatives at various levels have driven us to a point where not just organizations, but even each individual today is vulnerable. While baby steps are already being taken, India needs to come together and take leaps across segments to bridge this gap and live in a cyber-secure space. To tackle this issue, we suggest a 3 pronged approach to tackle these issues, urging Academia, Corporates, and the Government to take immediate measures to bridge the gap between demand and supply.

With multiple thousands of individuals being a part of the Academic sector, this area needs to be addressed first. Following curriculum that was decided a few years ago is no solution since the requirements of the industry changes at lightening pace. While a subject in cyber-security has been made mandatory by the UGC earlier this year, colleges are yet to adopt trainings and cyber-security subjects in their curriculum. Tackling this segment will help churn out large numbers of skilled professionals.

Technology is a way of life across businesses today and corporates focus on two important factors: increase in revenue and that their clients’ faith is intact. These could however, get affected by a simple leak of data or vulnerable software that could affect these and loss of even one could imply irreparable damage. Organizations need to get conscious and should focus on not just hiring skilled professionals, but also ensuring their teams are trained at regular intervals to meet the increasing demands of our ever changing industry.

The most important and critical is our Government. Industry data has proved that year on year the number of attacks on government sites has increased. The government requires maximum attention since any successful cyber-attack, no matter how minute, could endanger the entire nation. We need multiple levels of security in this sector. The immediate need is to hire talented professionals who not only mend and recognize breakaways and malicious attempts on our network and infrastructure, but also have the capability of building an impenetrable secure cyber wall that can prevent any possibility of our systems being compromised.

If these three segments are addressed with a zeal, India can definitely retain its title of being an IT superpower. We would like to end by the famous words of Jack Welch we often refer to: “If the rate of change on the outside exceeds the rate of change on the inside, the end is near.”
Appendix

a. Dissecting the talent across all the zones

Subject Matter Expert Percentage

This data reflects the percentage of the Experts available in the country across all the zones. Since there is a minuscule percentage of approximately 1% experts in the country, it depicts the immediate need for training the Trainable talent.

Trainable Percentage

The above chart reflects the pan-India Trainable talent, who, if provided with training facility, could be known as experts in the domain. This pool of talent could act as a catalyst in bridging the gap of the number of experts in the domain.
Ineligible Percentage

This chart reflects on the pool of talent which is Ineligible for the training on the information security domain. This further reflects that there is 86.3% of talent that is Ineligible for this domain.

---

End Notes


<table>
<thead>
<tr>
<th>Supporting Colleges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aligarh Muslim University</td>
</tr>
<tr>
<td>Dr. M.G.R. University</td>
</tr>
<tr>
<td>Nagpur Institute of Technology</td>
</tr>
<tr>
<td>Gandhi Institute For Technology</td>
</tr>
<tr>
<td>Thapar University</td>
</tr>
<tr>
<td>Dr.Mahalingam College of Engineering &amp; Technology</td>
</tr>
<tr>
<td>Parul Group of Institutions</td>
</tr>
<tr>
<td>Sikkim Manipal University</td>
</tr>
<tr>
<td>Amity University</td>
</tr>
<tr>
<td>Presidency College</td>
</tr>
<tr>
<td>Shri Datta Meghe Polytechnic</td>
</tr>
<tr>
<td>B.P. Poddar Institute of Management &amp; Technology</td>
</tr>
<tr>
<td>IIT- Varanasi</td>
</tr>
<tr>
<td>Anil Neerukonda Institute of Technology and Sciences</td>
</tr>
<tr>
<td>Karmavir Dadasheb Kannamwar College of Engineering</td>
</tr>
<tr>
<td>Krishna Murthy Institute Of Engineering &amp; Technology</td>
</tr>
<tr>
<td>Invertis University</td>
</tr>
<tr>
<td>Brilliant Group Of Institutions</td>
</tr>
<tr>
<td>Tulisiramji Gaikwad Patil College of Engineering and Technology</td>
</tr>
<tr>
<td>M.E.T Engineering College</td>
</tr>
<tr>
<td>Gyan Ganga Institute of Technology &amp; Sciences</td>
</tr>
<tr>
<td>Cape Institute Of Technology</td>
</tr>
<tr>
<td>Abha Gaikwad-Patil College of Engineering</td>
</tr>
<tr>
<td>Mahatma Gandhi Institute of Technology</td>
</tr>
<tr>
<td>Gyan Ganga College of Technology</td>
</tr>
<tr>
<td>Chennai Institute of Technology</td>
</tr>
<tr>
<td>Anjuman College Of Engineering &amp; Technology</td>
</tr>
<tr>
<td>Mahaveer Institute Of Science And Technology</td>
</tr>
<tr>
<td>Gyan Ganga Institute of Technology &amp; Management</td>
</tr>
<tr>
<td>Deccan College of Engineering &amp; Technology</td>
</tr>
<tr>
<td>Smt Radhikatai Pandav College of Engineering</td>
</tr>
<tr>
<td>Malabar College of Engineering &amp; Technology</td>
</tr>
<tr>
<td>SRMS College of Engineering and Technology</td>
</tr>
<tr>
<td>Gokaraju Rangaraju Institute of Engineering &amp; Technology</td>
</tr>
<tr>
<td>Dnyanprassarak Mandal's College of Arts, Science, Commerce, Management Studies &amp; Technology</td>
</tr>
<tr>
<td>Teegala Krishna Reddy College of Engineering &amp; Technology</td>
</tr>
<tr>
<td>SRMS Women's College of Engineering and Technology</td>
</tr>
<tr>
<td>Holy Mary Institute Of Technology &amp; Science</td>
</tr>
<tr>
<td>Government Polytechnic, Nagpur</td>
</tr>
<tr>
<td>Sreenidhi Institute Of Science and Technology</td>
</tr>
<tr>
<td>Hindustan College of Science &amp; Technology</td>
</tr>
<tr>
<td>-----------------------------------------</td>
</tr>
<tr>
<td>KCM School</td>
</tr>
<tr>
<td>Sant Singaji Institute of Science and Management</td>
</tr>
<tr>
<td>R.R.K. School</td>
</tr>
<tr>
<td>Hindustan Institute Of Technology &amp; Management</td>
</tr>
<tr>
<td>K.K.Wagh College of Engineering</td>
</tr>
<tr>
<td>SCSVMV University</td>
</tr>
</tbody>
</table>

**Disclaimer**

This document has been prepared in good faith on the basis of information available at the date of publication without any independent verification. EC-Council Foundation does not guarantee or warrant the accuracy, reliability, completeness or currency of the information in this publication nor its usefulness in achieving any purpose. Readers are responsible for assessing the relevance and accuracy of the content of this publication. EC Council Foundation will not be liable for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on information in this publication.

The recipient must not reproduce, disclose or distribute the information contained herein without the express prior written consent of EC- Council Foundation.
About EC-Council Foundation

EC-Council Foundation is a not-for-profit initiative by EC-Council to raise awareness of online safety issues for the global community while unifying global cyber defense. EC-Council Foundation’s mission is to unify global cyber defense by fostering collaboration and participation of online computer users to become advocates for safe on-line activities for youth and adults alike through education, and training programs. Cyber security statistics show that the majority of security breaches are: low in difficulty, take a long time to discover, are discovered by outside parties, and are perpetrated by outsiders. Through our programs we aim to stop malicious hacking at its core cause, while creating an opportunity for ethical hacking to be accepted and practiced without any discrimination, across all geographical boundaries for the purpose of understanding what it takes to protect and secure critical information and assets.

We foster child online protection and cyber security awareness through our programs. These include:

- Global CyberLympics
- The Cyber Post
- Code Uncode

EC-Council Foundation’s parent company The International Council of E-Commerce Consultants also known as EC-Council is a member-based organization that certifies individuals in e-business and information security skills. It is the owner and creator of the world famous Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), EC-Council Certified Security Analyst (ECSA), Licensed Penetration Tester (LPT), and numerous others that are offered in over 87 countries through more than 450 training partners globally. EC-Council has trained over 90,000 individuals and certified more than 40,000 security professionals.

For more information about the company please visit http://foundation.eccouncil.org/