BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 3, 2017

Editors' message

Dear Members,

We BCS Sri Lanka Section published a news letter on behalf of the SL Section as a mark of 20th year of BCS Sri Lanka Section. This is with the intention to communicate with the membership periodically and update the members on the activities carried out by the chapter. Currently we are releasing the 3rd newsletter for this year; we initially planned to release 2 newsletters for a year and gradually increase it up to 4 newsletters for a year. The support and encouragement given by the BCS Sri Lanka membership pushed us to fast-forward the target within 3 months.

In addition all our releases are targeted towards a specific special interest groups, volume 1 focused on eCommerce & Internet, Volume 2 focused on Application Development & Management and this Volume 3 is focused on IT Security & Cyber Law.

Thank you very much for all the encouragement and appreciation shared in this regard through email and in all other means. We hope you will continue to support us on this initiative. Please send us your feedback to nirmalan@bcssrilanka.org we will try our best to keep up with it.

Message from the Section Chairman

Beginning of the Competition Season

As you already know, BCS the Chartered Institute for IT Sri Lanka Section (BCSSL) has initiated the National Best Quality ICT Awards (NBQSA) 2017. This is the busiest time for the Sri Lanka Section as we embark on the organizing activities of the ICT Awards competition in the country.

This year NBQSA celebrates its' 19th anniversary and is expected to be organized in larger scale than ever before. Already the Applications are called and the deadline for submission of applications is 31st of July 2017. The organizing committee has already started the Tertiary category briefing sessions at different universities across Sri Lanka and will be followed by the Participants Briefing for the other categories.

The series of YPG events are been conducted with the participation of many members and other young professionals in the ICT industry. There are plans to organize similar seminars for senior professionals also in the near future. The sub-committee which organizes these activities require the support of many volunteers and BCSSL members who wish to do so are requested to contact the secretariat calling or sending an email.

Current Executive committee wishes to request all BCSSL members to utilize these opportunities to get involved either as volunteers in organizing activities or as participants of these events to network with professionals and other members.

Ruwan Amarasekara

Chairman – BCS the Chartered Institute for IT Sri Lanka Section

BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 3, 2017

Articles

TOP 8 MOST DANGEROUS BLIND SPOTS OF IT SECURITY

By
MR. DÁNIEL BAGÓ
PRODUCT MARKETING MANAGER at BALABIT Corp., USA.

"For all practical purposes, we can never secure or trust the … endpoint participants in any computing environment."

Amit Yoran, president of RSA, keynote speaker of RSA 2015 conference

The real message of the quote above is that minor and major security incidents are already part of an average day. Sony, Ashley Madison, Target, Uber and NSA are only a small snippet of those organizations that have suffered a very serious data breach recently. These stories also confirm the fact that attackers are, and will always be, ahead of us. It's not a matter of if these attackers will infiltrate our network. If our data is valuable enough for them, they will keep on trying until they get in – or they are already inside.

One of the key points of the success of attackers is that corporations have several blind spots in their IT environment. There is a common theme in most of these so-called blind spots: the activities connected to them appear absolutely normal in 99.99% of the cases – but although sometimes it seems that monitoring these potential security holes is infeasible, the experience of the last years prove that the most serious data breaches and security incidents originate from these security holes.

Top 8 most dangerous blind spots of IT security

1. 0-day & 0-hour threats
2. Lateral movement inside the network
3. Shadow IT
4. Business applications
5. Shared accounts
6. Database manipulation
7. Scripts running on personal accounts
8. File servers & file transfers

0-Day & 0-Hour Threats

According to Symantec's annual Internet Threat Security Report, 24 new 0-day vulnerabilities emerged in 2014, and the top 5 of them were left unpatched for a total of 295 days, compared to a total vulnerability window of 19 days in 2013. 0-day threats could be public enemy nr. 1 of IT security – every CISO knows how dangerous they can be to his or her protected IT infrastructure. Since threat prevention is very difficult and challenging using the current 0-day protection solutions, it is highly recommended to apply alternative forms of defense in the network.

Lateral Movement Inside The Network

Most monitoring solutions focus on authenticated logins to the company's IT system, not considering when an attacker might have compromised an employee's

trusted credentials and infiltrated the network. In this case, the attacker can freely move in the system for months. According to research by Ponemon and IBM, 90% of recent data breaches went undetected for over 3 months, which means IT security solutions shouldn't concentrate only on authentication.

Shadow IT

IT departments are unable to keep pace with the continuous flow of newly launched cloud and mobile applications. According to a study by IBM Security, about 33 percent of Fortune 1000 employees regularly save and share company data to an external cloud-based platform that the company cannot track. These GTD, notetaking, instant messaging or other kind of apps have become extremely popular among users, but in most cases, these are not approved by IT – users still find ways to install and use them. As IT departments do not know about them, do not pay attention what happens in these applications and can't prevent the leakage of valuable company data from there.

Business Applications

Business applications – such as SAP and others – play a crucial role in the everyday operation of almost every company. These contain a huge amount of valuable information ranging from the financial data to client lists – even traditional IT security defenses are unable to monitor what happens in these systems, e.g. which privileged user leaks out what kind of important information using these applications.

Shared Accounts

"Three can keep a secret, if two of them are dead", as Benjamin Franklin famously said, and it's true for shared accounts as well. The cornerstone of most security policies is to have personally identifiable accounts and only use shared accounts when it's absolutely unavoidable and do it in a controlled way.

Database Manipulation

Databases contain a lot of valuable company information – they are home to almost all sensitive information from bank account numbers of employees to the detailed lists of invoices issued by the company. Unfortunately, most enterprises do not have reliable methods to detect when someone manipulates their databases.

Scripts Running On Personal Accounts

When a sysadmin automates some tasks he has to perform regularly and allows a script to use his own credentials, he creates a huge security risk. If an attacker finds a way to hack the script (and such ad-hoc developments are often prone to trivial attacks like SQL or shell injections) or gains access to the stored credentials the script is using, he gains access to all the services the admin has access to.

File Servers & File Transfers

Besides databases, file servers are the second most important sources of critical data. And similar to databases, traditional IT security solutions do not defend these very well, do not pay extra attention, for example, to the transfer of sensitive files.

A defensive strategy that is based purely on access control, incident management and identity management is not sustainable. The complexity is overwhelming and the constraint on business is unacceptable. Besides, the greatest risk usually comes from someone who has gained access and is able to abuse privileges already granted.

Experts agree that the new perimeter, where we have to focus, is our users. They are the new focus of our security measures instead of the infrastructure. Users present too big a challenge for most of the current security solutions, as the required level of data, analytic capability or the contextual information to catch their potential malicious activities isn't available.

Traditional IT security solutions are mostly target known threats – but these 8 blind spots prove that the most dangerous threats frequently arrive in unknown forms. User Behavior Analytics is the next generation of IT security solutions, which is able to identify unknown threats by monitoring users and gathering logs of system and application activity. The continuous and real-time analysis of these activities will minimize the time to detect, assess and prevent data breaches by thorough and rapid investigation.

IMPORTANT GLOBAL CYBERLAW TRENDS 2017

BY

PAVAN DUGGAL
ADVOCATE, SUPREME COURT OF INDIA
PRESIDENT, CYBERLAWS.NET, HEAD, PAVAN DUGGAL ASSOCIATES, ADVOCATES

The year 2017 promises to be a year of tremendous developments as far as Cyberlaw jurisprudence is concerned.

The year 2017 is likely to build upon the foundations of Cyberlaw jurisprudence which has been placed at a strengthened position in the preceding years especially in the year 2016. It is hard to crystal gaze and predict specifically. However, on the basis of the information available, some broad trends of Cyberlaw jurisprudence can be detected on the horizon.

Cyber Security Legal Approaches

The first biggest trend on Cyberlaw jurisprudence that the year 2017 is likely to see emerging cyber security legislative instruments and legislative approaches. Cyber security over the last few years has ceased to become a merely technical issue. On the other hand, it is becoming a very critical Cyberlaw, policy as well as regulatory issue. Different countries have already started coming up with different legislations and policies concerning cyber security. The year 2017 is likely to see more countries coming up with detailed legislative frameworks as also national policies impacting cyber security. The difference of approaches, which the specific countries will make, will be dependent on the peculiar challenges that they face from time to time. Some countries are likely to introduce significant cyber security laws while other countries are expected to go through soft legislations route, by coming up with national policies and appropriate guidelines to govern cyber security ecosystem and the roles, duties and responsibilities of respective stakeholders therein.

Bilateral Cyber Security Agreements

Another important trend in Cyberlaw jurisprudence that is likely to evolve will be increased adoption and execution of cyber security bilateral cooperation agreements and arrangements. Countries across the world have recognized that there is lack of an international Cyberlaw on cyber security. Countries further recognized that cyber security is a global paradigm and that it would require global approaches to be effectively dealt with. However, countries are also appreciating that it will take some time for international Cyberlaw frameworks to be put in place. Hence, more

and more countries are likely to go in for bilateral cyber security arrangements and cooperation agreements as also anti-hacking

agreements with other countries. These arrangements and bilateral treaties would aim to strengthen cooperation mechanisms between countries and provide for more sharing of information concerning protecting and preserving cyber security as also information concerning cybercrimes. These bilateral agreements and arrangements are further going to contribute to the crystallization of key international principles impacting Cyberlaw and cyber security which countries could agree upon, thereby contributing to the development of international jurisprudence concerning cyber security law.

International Commonly Accepted Principles And Denominators Impacting Cyberlaw

The year 2017 is further likely to see more discussions and debate upon coming up with international legal framework impacting cyberspace. The absence of an international cyberlaw has necessitated that countries look at common legal principles impacting the regulation of cyber issues at a global level.

The year 2017 is likely to see further discussion moving in the direction of distilling the international commonly accepted principles and denominators impacting Cyberlaw which could then be part of an international treaty. The Author has already mooted the idea of the need for having in place an International Convention on Cyberlaw & Cybersecurity in 2015 itself. As the world begins to see more global threats emerging to the security and stability of the Internet, there is likely to be more calls for coming up with common minimum denominators and principles of international law which could then contribute in the direction of an International Convention on Cyberlaw & Cybersecurity.

Legislative Approaches Governing Emerging Cybercrime

Another important trend that the year 2017 is likely to see is the increasing attempts at legislative approaches aimed at regulating emerging kinds of cybercrimes. Cybercrimes are continuing to proliferate with each passing day. Newly emerging kinds of cybercrimes like ransomware have already impacted industries worldwide. The advent of the Darknet and cyber criminals activities originating therefrom provide further legal headaches and challenges for law enforcement agencies across the world. In this context, the year 2017 is likely to see more movements in the direction of strengthening national legislative approaches and legal frameworks regulating cybercrimes. Meanwhile, the year 2017 is likely to see far more calls for closer cooperation at the international level concerning cybercrime information sharing and strategies for getting effective prosecutions in cybercrime matters.

Darknet Jurisprudence

The year 2017 is further likely to see more work happening on developing the legal jurisprudence concerning the regulation of cyber criminal and illegal activities done on the Darknet. Hence, there is a need to work on attribution related principles concerning cyber criminal activity on the Darknet.

Principles Impacting Attribution Of Cyber Criminal Activities In Cyberspace

Another important significant Cyberlaw jurisprudence trend that is likely to emerge in the year 2017 would relate to crystallizing and developing principles impacting attribution of cyber criminal activities in cyberspace at

international level. Internet has made geography history but the same boundary-less medium is sought to be regulated by national

legislations. Consequently, internet jurisdiction continues to be a big legal problem.

Internet Jurisdiction

More work needs to be done on tackling the legal challenges raised by the Internet jurisdiction in the year 2017. Cyber criminals often hide behind the anonymity on the Internet as also the complex challenges raised by Internet jurisdiction to escape exposure to potential prosecution. Globally, the discussion is likely to be distilled further in the direction of evolving strong and sound legal principles impacting attribution of criminal activities on the Internet.

Internet Of Things Legalities

The year 2017 is further likely to see more work happening to develop the legal principles governing Internet of things and transactions made thereon. With 24.8 Billion[1] number of devices expected to get connected with Internet of things by 2017, cyber security and protection of privacy become important vectors on which legal frameworks need to be developed. As the year 2017 witnesses more adoption and usage of Internet of things, it is also likely to see more work on the legalities and legal principles governing Internet of things, more so in the context of cyber security, personal and data privacy as also data protection issues connected therewith.

Data Protection In A Ubiquitously Connected Internet

The year 2017 is further likely to see more discussion and debate on how to ensure data protection in a ubiquitously connected Internet. Countries may look at different approaches prevailing in the global scenario to modify and remodel existing data protection strategies aimed at protecting data effectively and efficaciously.

Consumer Protection Issues

As more and more consumers join the digital bandwagon at the global level, we are likely to see further jurisprudence evolving concerning consumer protection issues in cyberspace. Consumer protection issues are already marked as important issues in some jurisdictions while in other jurisdictions, consumer protection is virtually non-existent. The year 2017 is likely to see further development of jurisprudence impacting consumer protection in the year 2017.

Blockchain Legalities

The year 2017 is further likely to see more work being done on the legalities pertaining to blockchains as a transformative technology. With increased adoption of blockchains in banking, financial and other sectors, there is a need for more work to evolve jurisprudence concerning blockchains at a global level. The further adoption and strengthening of usage of crypto currencies across the world further means that work on the legal challenges raised by crypto currencies need to be done in 2017 so as to enable countries to have common minimum platform of regulating activities done using crypto currencies.

Social Media Jurisprudence

Social media will continue to rise in 2017. New social media platforms are increasingly engaging the attention of the netizen

[1] https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

community. The legalities concerning social media jurisprudence require more discussions and debate. There is an urgent need to protect women and children on social media from unwarranted exposures and influences and Cyberlaw needs to play a significant role therein

Cyber Radicalization And Cyber Terrorism

As cyber radicalization and cyber terrorism continue to grow unabated, the year 2017 is likely to see more focus on coming up with national and international frameworks to effectively regulate the same. Counter narratives to deal with cyber radicalization, would require enabling legal support from legal frameworks all over the world. Cyber terrorism jurisprudence would need to be expanded in 2017 to cover the emerging new activities being engaged in by cyber terrorists all over the world.

Regulation Of Intermediaries As Data Repositories

The year 2017 is likely to see more focus on the regulation of increased role of intermediaries and service providers as data repositories , with increasing compliance and due diligence requirements. Countries across the world are increasingly likely to examine the important complex role played by the intermediaries in the cyber ecosystem and put more responsibility on such data repositories concerning cyber security as also protection of third party data.

Data Protection And Privacy

The year 2017 is further likely to see the focus on protecting and preserving data as also personal privacy. In that context, the year 2017 is likely to see increased discussion and debate on how to protect and preserve data and personal privacy in accessing consumer data.

Encryption Balancing

Since encryption is a very important subject, the year 2017 is likely to see further calls for need to develop legal principles in such a manner which can help create golden balance between protection of privacy using encryption and the intrinsic rights of the sovereign states to have access to backdoors.

Individual Rights Versus Cyber Sovereignty

The year 2017 is further likely to see a conflict emerging between protection and preservation of individual rights on the Internet and increasingly bigger ambit of cyber sovereignty of sovereign nations. As freedom of speech and protection of fundamental rights on the Internet engage the centre-stage attention in different jurisdiction, Cyberlaw jurisprudence is likely to be called upon to develop robust effective and efficacious principle which can help balance both the competing demands from different stakeholders in a delicate manner.

Norms Of Behaviour In Cyberspace

The year 2017 is further likely to see more discussions on the applicability of international law to cyber warfare issues. Discussions around rules and norms of behavior in the cyberspace expected from all stakeholders in the cyber ecosystem will increasingly engage the attention of the relevant stakeholders.

The aforesaid are some of the important trends in Cyberlaw jurisprudence that one can detect emerging in the horizon. Needless to say, I am not a Soothsayer and it is not possible to predict comprehensively. However, on the basis of the developments that have taken

place in the year 2016 and earlier years, it is expected that the aforesaid issues will increasingly become more significant in terms of their importance and would further help in contributing to the evolving Cyberlaw jurisprudence at global, regional and national levels.

It will be interesting to see how the jurisprudence concerning Cyberlaw issues, aspects and subjects will actually evolve in a robust and efficient manner in the year 2017.

National Best Quality ICT Awards (NBQSA)

Since 1998, the National Best Quality Software Awards (NBQSA) has been the only National competition of its type held in Sri Lanka for the ICT Industry. It has provided a unique platform and opportunity for local organisations and individuals to display and benchmark local ICT talents to the business industry and the world. NBQSA stands as the "*Seal of Excellence"* in the ICT industry and serves as an effective mode to gain international recognition for locally developed ICT products, enabling them to successfully compete in the global market.

The NBQSA journey is a proud initiative of BCS The Chartered Institute for IT Sri Lanka Section as a way and means of giving back to the ICT Industry of Sri Lanka. From its humble beginnings with very nominal no of applications for the first year, NBQSA today draws more than 200 applications in its respective categories and most of the submission by the well-known prestigious companies in Sri Lanka as well as the startup levels due to its powerful awareness campaign carried out by the committee and has reached the each corners in the country.

But that's not all, NBQSA also recognises and encourages the young local talents who are great innovators and entrepreneurs in the making and will recognize and award students who have showcased exceptional achievements in Technology Usage as well as Business Potential.

The competition is open to more than nineteen categories and will also recognize;

- An outstanding personality for the invaluable services rendered to the development of the local ICT Industry for an extended period of time with the 'ICT Lifetime Achiever Award'
- A budding entrepreneur who will be recognized for his or her effort for venturing into the organizational development in an ICT organization with the 'ICT Entrepreneur of the year Award'
- A public sector organization in recognition and appreciation of the effort rendered towards the introduction, nurturing and development of ICT environment to provide better quality services to the Citizens in Sri Lanka with the 'Public Sector Most Outstanding ICT Achievement Award'

The unbiased judging process is carried out by a distinguished Panel of Judges consisting experts from diverse disciplines such as IT, Engineering, Management, Accounting, Marketing etc. representing both the Private sector as well as Academia. In addition, a well-tested online evaluation system has also been introduced to the NBQSA since 2014 to uplift the efficiency of the judging and scoring and the system was certified by the APICTA judges at the competition held in Sri Lanka (APICTA 2015).

NBQSA as the only recognised award in the ICT industry in Sri Lanka has proven beyond any doubt that the products recognized here are indeed the best of the best developed in Sri Lanka and suitable for participation at an awards ceremony in the caliber of the prestigious Asia Pacific ICT Awards (APICTA) continuously for the past 16 years. The NBQSA programme is well aligned with the APICTA competition and the evaluation and decisions made by the distinguished judging panel are some of the best compared to the other member countries of the APICTA.

Finally, after many years NBQSA has been identified as the trendsetter to many associations that recognition is one of the most successful key factors in to evolution of any industry.

Vajeendra S Kandegamage
Chairman – NBQSA 2017

BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 3, 2017

YPG Activities

Young Professionals Group (YPG) of the BCS, The Chartered Institute for IT Sri Lanka Section is conducted the following YPG sessions.

May 2017 - People Engagement Through Gamification of Working by Aruna Dayanatha

Mr. Dayanatha explained how to optimize the people engagement to the work through computer games and gaming platforms. He also expressed his view on how the Information Technology plays significant role in the is endeavor and he mentioned that Industry is learning from games and taking the gaming elements to business world and peruse the engagement of people, as customers or employees. About 50 members have participate at this event.

June 2017 - Entrepreneurship, Risks and Opportunities in the Australian Market by Professor Kevin Fynn

YPG in association with Curtin Alumni Sri Lanka Chapter has organized an event to enlighten the professionals in Sri Lanka on the Risks and Opportunities in the Australian Market. Professor Kevin Fynn is veteran entrepreneur and researcher who was a part of many startups who expressed his views and shared the experience on his journey.

He also gave invaluable tips for people who are looking at opportunities in the Australian Market.

BCS the Chartered Institute for IT – Sri Lanka Section
Member News letter
Volume: 3, 2017

Upcoming events of BCS SL Section

NBQSA 2017

Events Schedule

Judging process (Commercial)	17th to 22nd August
2nd Round evaluations (Commercial)	8th to 10th September
Judging process (Tertiary)	1st to 15th August
2nd Round evaluations (Tertiary)	26th to 27th August
Lifetime achievers & ICT Entrepreneurship Evaluation	September
NBQSA 2017 Award Presentation	6th October 2017
Asia Pacific ICT Awards competition will be held in Dhaka, Bangladesh.	6th to 9th December