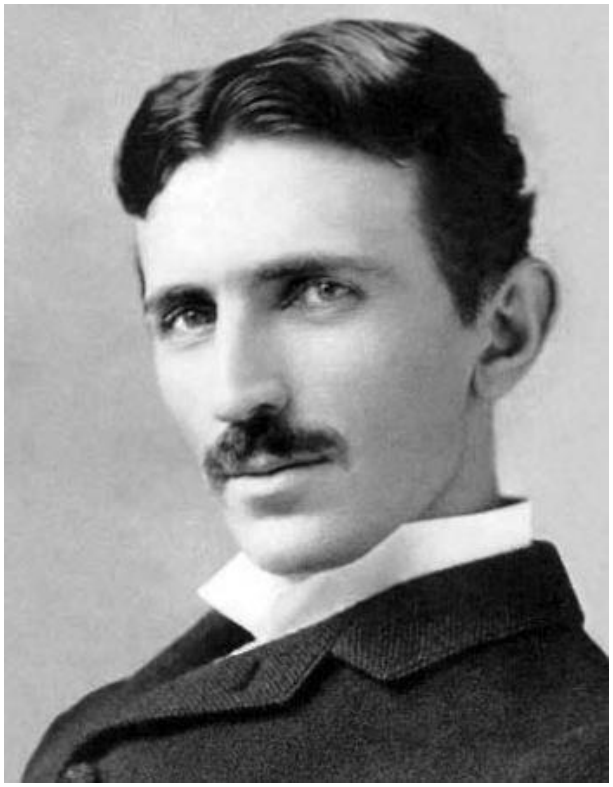
IEEE New York Monitor

Advancing Technology for Humanity

June 2018, Vol. 65, No. 6



Our virtues and our failings are inseparable, like force and matter. When they separate, man is no more.

Nikola Tesla

1856 – 1943

Principal officers of the IEEE New York Section 2018

Chair: David K Horn

Vice Chair, Chapter operations: Robert M Pellegrino

Vice Chair, Section Activities: Wilson M Milian

Treasurer: Thomas Villani

Secretary: Amy Batallones

EDITOR NY MONITOR: DR. AMITAVA DUTTA-ROY

Currently, the New York Section of IEEE comprises of the following Active Chapters of the IEEE Societies:

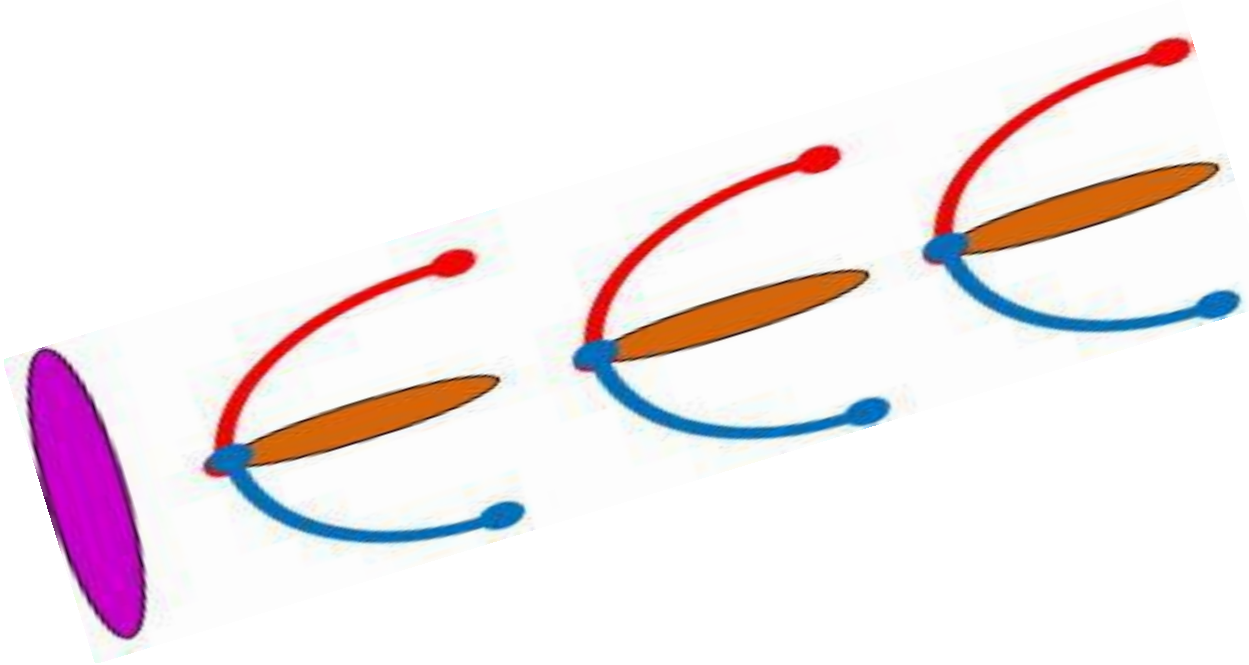
- Computational Intelligence Society
- Computer Society
- Communications Society
- Technology Management Society
- Engineering in Medicine and Biology Society
- Instrumentation and Measurement Society

- Power and Energy Society
- Industrial Applications Society
- Solid State Circuits/Electron Devices Societies
- Systems, Man and Cybernetics Society
- Vehicular Technology Society
- Broadcast Technology Society

&

The following Affinity Groups as defined by IEEE

- Consultants' Network
- Life Members Affinity Group (LMAG)
- Women in Engineering
- Young Professionals



QUICK DATE CHECKS FOR NY SECTION EXCOMM MEETINGS

The following are the presumed dates for the 2017 Executive Committee meetings at IEEE NY Section (unless otherwise notified in advance, always held on the second Wednesday of the month)

~~10 January~~
~~14 February~~
~~21 March~~
~~11 April~~
~~9 May~~*
~~13 June~~
No meetings during the months of July and August
12 September
10 October
14 November
12 December

****

Unless otherwise notified, all ExComm meetings are scheduled for 12:30 pm at the ConEd Building, 4 Irving Place, New York. All members of the New York Section are invited to participate in the ExComm meetings. However, for reasons of security controlled by ConEd, the owner of the venue, all members desirous of attending any ExComm meeting must notify the Section chair. Thank you for your understanding

Did you know that the IEEE is also heavily involved with the philanthropy of IEEE Foundation by supporting efforts in STEM education, in improving public health, conservation of energy, and disaster relief in many parts of the world?

Why should you write in the NY Monitor?

Why should you write at all?

Amitava Dutta-Roy, Life Fellow, Editor

Are you a member of the IEEE, and of good standing? You have been so for years, right? I assume that your reply is an assertive "yes." If that is so, then let me ask you a simple question: have you ever read the constitution of the IEEE by which we are all guided for our actions relevant to IEEE that we undertake? No? Then let me tell you that the IEEE has six major boards for overseeing its operations in various sectors of its endeavors. One such major board is known as the Publications Services and Products Board (PSPB) and, in a way, it happens to be the most important. Why? Let me explain!

If you did not know, publications — Transactions and magazines (e.g., Communications Magazine) of IEEE Societies, Proceedings of the IEEE (a highly coveted and learned journal read mostly by active researchers, supervisors and technical directors), the newsletters of Sections located worldwide and their bulletins are a major source of revenue for our IEEE. The organization produces over 30% of the world's literature in the electrical and electronics engineering and computer science fields, publishing well over 100 peer-reviewed learned journals. Want some facts? In 2017, the IEEE published more than 50, 800 articles that generated 42.4% of the total revenue of the IEEE. Any publication of repute that proudly displays the publisher's logo is naturally expected to comply with a set of established guidelines. In our case, the publications — either in print or posting on the Web — use the IEEE logo are expected to be guided by the 132-page Manual of Operations of the PSPB. (Only the Spectrum magazine, because of historical and strategic reasons, falls outside the scope of PSPB.)

The other five IEEE boards, in alphabetical order, are: Educational Activities Board (EAB), IEEE-SA Board (Standards Association), IEEE-SA Board (IEEE-USA), Member and Geographic Activities Board (MGA) and Technical Activities Board (TAB). As their names indicate they have their functions also clearly determined by the IEEE Board of Directors.

Let's revert back to the IEEE Constitution that states: "Publication Services and Products Board (PSPB) formulates and recommends information-related published services and products policies to the IEEE Board of Directors, establishes and maintains standards and procedures for IEEE information dissemination, recommends policies and best practices as they relate to the IEEE website, and otherwise coordinates and assists with activities of IEEE and its various organizational units. The PSPB Operations Manual (PDF, 1 MB) contains additional information related to PSPB." The five IEEE boards may are certainly free to publish their journals or proceedings of conferences but everything must conform to the rules of PSPB manual.

Many of you may not attach much importance to the Section newsletters. To you such online postings are just calendars, to check what meetings and events are being scheduled for the month. I bet those who think in that way are not cognizant of the hard work that is required to continue with the posting of a newsletter month after month. They may not

perceive that a newsletter not only must comply with the requirements of the PSPB rules but also offer a critical mass of the contents to its readers. I must draw those readers' attention to the fact that the PSPB makes a noticeable distinction between a bulletin and a newsletter. The newsletters are bundled into the same group as other publications and postings of the IEEE. As mentioned above newsletters are not bulletins and are allowed and even encouraged to post technical articles general interest to the heterogeneous membership of the IEEE and the communities surrounding us. (Articles published in newsletters do not require peer review and for this reason the latter are known as nonrefereed.) At IEEE we are involved in STEM education, standardizing new technologies, fostering professionalism and even helping with philanthropy. Consequently, we deserve our non-taxable status and let the world at large know this. This is an unwritten mandate we all have. What would be the way of telling people about *ourselves* other than by writing and posting our stories online that all can easily read on the web? So, why don't you write about a new project you have been working on and write about your own experience with your job or with the IEEE? The PSPB manual gives the newsletter editors of free hands to accept and post an article compatible with the general spirit of the IEEE. We have no peer reviews. The editors have the final authority of the contents. But that freedom comes with a heavy price tag. Like any other refereed publication, the editors of (nonrefereed) IEEE newsletters must make sure that and article is compatible with the high standards of IEEE:

- The articles contained therein are **relevant** to the IEEE. An editor can accept an article on an improvement on Dolby system but the telemetering of the pH in a vineyard could be far cry unless the technology involves something new as to the sensitivity of the sensors or the auto-control of watering of the grapevine. Herein come the experience and interest of the editor
- Any decent publication should have a **critical mass** of contents. I would not expect you to open Web pages and see just the list of contents or the calendar of the month. The editor should have the experience to judge what constitutes a critical mass
- **Timeliness** is important. We cannot delay publishing an article or information on an event that is time-sensitive. That would be the responsibility of the bulletin if that exists at all. (On some occasions, I must admit, the Monitor was posted late. But it could not be posted only with a calendar of events.) Hence, if you wish to publicize your chapter event please do send the relevant information in time with all necessary details. If you do it in pdf format the entire page will be snapped and be posted as an image.
- **Impartiality** is paramount in our postings. The newsletter editor must look and edit the articles so that there is no bias from any side. We cannot take sides in the Section, Region or mainstream IEEE elections. We can just publish the names of the candidates.
- **Legal** questions may arise not only regarding Monitor but with any publication. An author may write about a technology that is protected by a non-disclosure agreement. The article may have been a copy of an article by another author (plagiarism). It may be a copy of another article by the same contributor but copyrighted and published elsewhere though posting of an article or image previously copyrighted by another IEEE publication may be allowed. My personal understanding is that we cannot post any anonymous contribution. These are thorny questions and the editor of a newsletter will be well advised to check any article submitted to the Monitor for the legalities.

Thus, you can understand that the responsibilities of an IEEE newsletter editor are heavy. That is why PSPB demands that the editor of a newsletter must be a member of the IEEE who is willing to assume adequate responsibilities. My plea is that do not pooh-pooh your newsletter. Rather, collaborate with and contribute to your Section newsletter and leave a mark.

Of course, like many other things in life, the PSPB rules are not perfect. We still do not have a definitive stylesheet like most reputable publications such as our own Spectrum magazine, Times (London), NY Times, the Economist, the New Yorker or MLA and the Chicago Stylesheets. Hence, we do not know if we should include Professor, Dr., Mr., Ms. or Mrs. with or without the period sign in front of a name. Should we include the grade of membership after an IEEE member's name, especially when many of our members do not want to add the prefix "Life" to their

membership? The IEEE editors' lives would be easier if we had our own uniform stylesheet.

From my own experience of writing in the Spectrum magazine, Communications Magazine and Proc. IEEE and the still the citations they get from many parts of the world writing leaves an indelible reference though, at my age, it really does not add any extra credibility. But for the younger brothers and sisters in our profession it could be important, especially when they apply for jobs or contracts. It is commendable that as a volunteer you may be helping your Section and chapter in organizing presentations and networking events. But do try to write and make sure that you are never forgotten. In future, you can always refer to your own work in your resume and biodata while writing in other articles. Don't just talk the talk but walk (write) the walk (text)! You do *not* need the permission of anybody in the IEEE to write as long there is no objection from your superiors, e.g., professor, supervisor or the marketing department of the employer. Write, submit and leave it to the editor of the publication to help you.

Have I written too much about an IEEE publication? But I had to do this for encouraging you to be a contributor to IEEE publications. The Monitor is a good starting place.

What you could expect to read about in this edition of the Monitor?

Now I can describe what you can expect in this edition of the Monitor. We have received three interesting articles worthy of publication here. The first describes a wee bit of history of technology at, literally, our doorstep and in this city. It concerns Nikola Tesla, a Croatian-American physicist and engineer. Tesla was born in 1856 in a country, then under the Austrian empire and now known as Croatia. Though the name of Tesla has now been made famous by the electrically driven car developed by Elon Musk's auto company he is credited with inventing many technologies that involved static and moving electricity. New York City was his base where he died in 1943. Do we know what valuable contribution Nikola Tesla made to the electrical power industry? Read all about it in the article by Joe Cunningham, a noted New York-based historian of technology. He has written books on history of technology and published in our own IEEE's P&E magazine and in this newsletter as well.

The second article is about digital forensics. I had heard about this term but was did not quite know what it meant. These days of hacking, phishing misrepresenting of identity and snooping in general wouldn't it be nice to know the first steps to take for catching the thieves? That is why I, thanks to Fordham University Professor Frank Hsu, the chair of Computational Intelligence Society's NY Chapter, attended an international conference on cyber security sponsored by Fordham and Federal Bureau of Investigation (FBI) where Ashim Kapur of New York-based Stroz Friedberg, a firm specialized in the dealing with digital crimes and forensics. Kapur gave am introductory talk om the topics and though I do not know everything about them I am at least familiar with the terms. We thank Kapur for contributing this article.

The third article is on ambient intelligence and it is written by a familiar hand at IEEE. The author Professor Vincenzo Piuri is a distinguished educator and researcher at the University of Milan, Italy. He is also a visiting professor at two US and four European and Asian universities. His research interests are in intelligent systems, neural networks, pattern recognition, machine learning, signal and image processing, fault-tolerant, and digital architectures. At IEEE, Prof. Piuri has held committee positions in the PSPB and TAB where he also served as its VP. He has been a member of the IEEE for the last 34 years and now is its Fellow. In this short article, Piuri introduces us to the concept of environment and how it could be made intelligent so that it autonomously serves the individuals and as well as the collectively society inside it. The topic is not all that easy to understand. However, the author writes his introduction in a plain language easily understandable by our heterogenous membership. The tutorial shows us the direction in which artificial intelligence is progressing.

ENJOY YOUR READING!

New York City: The Cradle of Commercial Utility Power

Joe Cunningham

Popular history of New York has it that Thomas Edison's Pearl Street generating station and the half-mile stretch of lower Manhattan it illuminated was the beginning of deployment of commercial utility power and the story ends there. Little attention has been paid to other installations. Among them totally forgotten is the Excelsior Power Company generating station of 33 Gold Street, two blocks west of the Edison plant. It initiated the supply of commercial utility power for industrial motors in the factories and commercial establishments of the area of New York City and in 2016 it was designated a landmark by the City Landmarks Preservation Commission.

A few blocks away, Edison had installed his first "Annex" station in a commercial building located at 60 Liberty Street. The Annex scheme provided additional power with minimal space requirements by the use of steam from the boilers of the building in which it was located. Though a short-term approach, such annex stations met the intense demand for electric power in dense business zones.

Across the street, at 59 Liberty Street, the Safety Electric Light Company established its home office and the company started supplying alternating current and later became the United Electric Light and Power Company, a future Westinghouse holding. It was destined to perfect urban distribution of alternating current and pioneered the automatic network that replaced dc distribution.

Beyond power stations, there were developments which set future trends across the nation. The most significant of all was just a block farther west, on Liberty Street. There at 89 Liberty Street, the legendary electrical inventor and researcher Nikola Tesla began his own career in the United States. A native of Smiljan, Croatia, he was educated in Europe and had tried to interest potential backers in his invention of the induction motor and polyphase alternating current system. Upon emigration to the U.S. in 1884, he worked for Thomas Edison but made no headway in obtaining any interest in his concepts. After a year of odd jobs and some development work on arc lamps for several investors, he succeeded in attracting financial support to his ideas. Those investors helped him in his first commercial venture, the Tesla Electric Company, and with this support he established his small lab. It was there that he constructed a patentable alternating current system and sold the patent rights to George Westinghouse who then placed it on the market with a public demonstration at the Chicago Columbian Exposition. That exhibit changed the opinion of the Niagara Commission to favor alternating current for the Niagara Falls hydroelectric plant and initiated the first regional power transmission that truly launched the "Electrical Age."

To be acceptable, any new technology must be safe and the generation and use of electric power were no exception. Around the corner and a bit south of Tesla's lab the in the offices of the New York Board of Fire Underwriters was written what is believed to be the world's first electrical code. From an initial set of seven rules it became basis for the National Electric Code. Regardless of where in the nation new electrical projects matured, their ancestral trail almost always traces back to a tiny section of Manhattan better known to the public as the Financial District. The area received that name when

stock traders in the 1700s established their offices. A century later; drawn by the need to attract investment capital electrical pioneers gravitated to this very district.

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

INTRODUCTION TO CYBERSECURITY

Ashim Kapur *

Barely a day goes by that we don't read about a cybersecurity incident in the news, whether it's the point of sales (POS) systems compromised at a store, or personally identifiable information (PII) stolen from a server hosted at a health care establishment. In the face of nefariously evolving cyber risks, organizations need a robust cybersecurity program that enables them to proactively mitigate their cyber risk and increase their level of resilience when they are under attack or experience a compromise.

The digitization of almost every aspect of business, combined with the increased connectivity between people, devices, and organizations, has created a complex security landscape, leaving enterprises vulnerable to cyber risk. To remain competitive, companies continuously strive to enhance their customer experiences by supporting a multitude of connected endpoints, ranging from mobile devices (for instance, online banking apps) to automobiles.

While driving innovation and revenue, every company activity, be it a merger or acquisition, or the implementation of a new software or hardware, also leads to a dramatic increase in cyberattacks .

The threats facing organizations continue to widen in scope and scale, with sophisticated adversaries, from organized hacking groups trying to propagate their political views, to nation states seeking to gather information on intellectual properties (IP) from private industry competing against state-sponsored industries, to criminals seeking financial gains, and even insiders operating within an organization's perimeter. The most common cybersecurity attacks include:

- **Unauthorized Access/Data Breach** – Accessing or using someone else's account without consent to access or steal sensitive information, such as PII Payment Card Industry (PCI) or Protected Health Information (PHI) data, usually for monetary gains.
- **Phishing Campaigns** – Attacks in which a fraudster impersonates a legitimate company, customizing the attacks based on target information, in order to steal PII funds or login credentials. Consider a situation where, through business emails or fraudulent attacks as genuine orders from the CEO fraudster pretends to be a member of the institution and requests a transfer of funds.
- **Ransomware** – A type of malware that locks files, data or a PC itself and extorts money from the user in return for access. Some ransomware, like Petya and WannaCry, are worms that propagate within a network, infecting and encrypting files with a specific file extension. The latest breeds of ransomware target the internet of things (IoT), affecting the functioning of sensitive systems, such as on-board telematics for a self-driven vehicle, or even a pacemaker.
- **Advanced persistent threat (APT)** - A stealthy network attack in which an attacker gains access to a network by exploiting

unpatched vulnerabilities and maintains undetected presence within the network in order to harvest information over a long period of time or cause damage to the network or organization. Such an attack often target organizations for corporate espionage or state-sponsored political motives.

- **Distributed Denial of Service (DDOS)/ malicious code/ vandalism** – An attacker overwhelms the bandwidth of the target institution in order to prevent normal functioning. Such attacks include Botnet zombie machines or other attack vectors like a Trojan, virus, worm, or malicious script that disrupts the normal operation of a system or network.

To protect themselves in an evolving threat landscape, organizations need to apply a combination of proactive cybersecurity measures, and also manage the reactive elements, including digital forensics and incident response. Whether building these capabilities in-house or constructing a program with external experts, a solid understanding of the different threads in a cybersecurity program is critical.

Proactive Cybersecurity

Given the changing nature of cyber threats, no organization can be 100 percent secure. Instead, they should aim to establish and maintain cyber resilience, in order to decrease the likelihood of falling victim to an attack at the first place, and to reduce the damage and downtime in the event of an attack. To achieve this, organizations must take a proactive approach to cybersecurity, focused on protecting IP and other commercially valuable assets, and increasing readiness should such an incident really occur. Some critical elements of a program include:

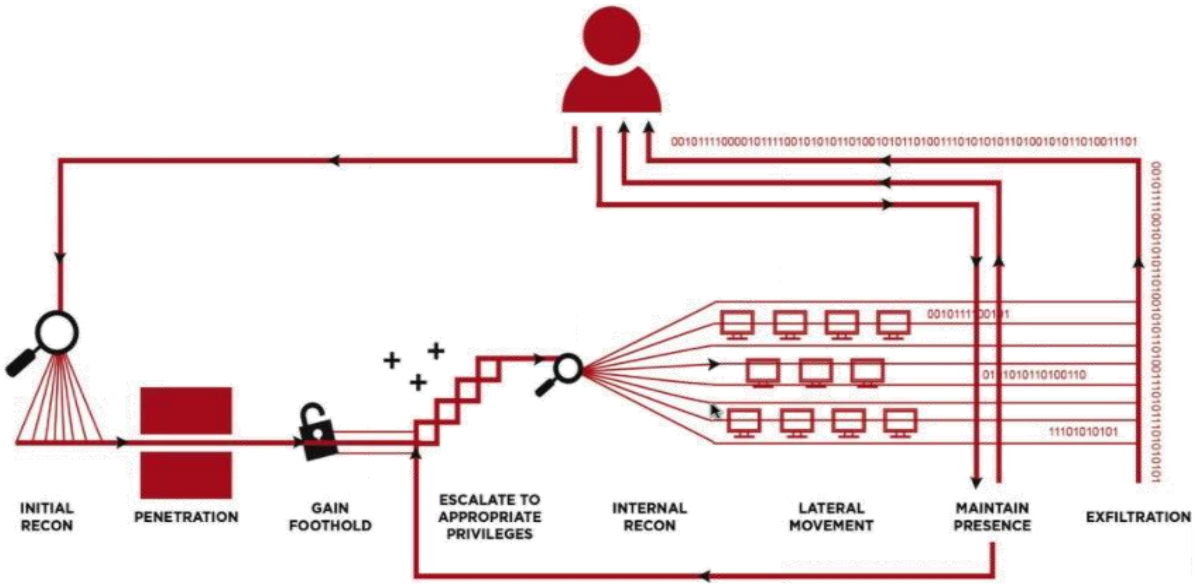
- **Conduct a security risk assessment.** The first crucial step in a proactive security program is to identify threats and vulnerabilities, by conducting a comprehensive information and technical security risk assessment of the current network security posture. These can then be prioritized and remediated based on the level of risk they pose to the organization and its most critical assets.

- **Implement an incident response plan.** In order to facilitate and be equipped to handle an incident, organizations must have an incident response readiness plan in place. The plan should be based on a detailed understanding of the organization's current cybersecurity environment, identifying current incident response capabilities, performing a gap assessment, and implementing improvements. The plan may also be evaluated against industry standards for response readiness. It must also be regularly tested and updated, and designate a multidisciplinary team, including IT, security, communications, HR, legal, and others.
- **Board Advisory and threat simulation.** For a cyber-resilience program to be effective, it has to be accepted by the ranking members of the organization. Advising and educating the senior members of the organization by performing a tabletop exercise simulating an attack will help raise awareness of the organizations' capabilities and shortcomings to handle the incident and improve the overall effectiveness of the cyber security program.
- **Conduct penetration testing.** Given the fact that the attack vectors or attack trajectory changes daily in cybersecurity, organizations need to commit to a continuous process of improvement. One way of assessing the current cybersecurity status is by conducting a 'Penetration Test' (Pen Test), which looks at the current network security setup to identify vulnerabilities that an attacker could exploit to access the organization's critical assets such as IP, client data, PHI/PII.

- **Reactive Cybersecurity – Incident Response**

Incident Response involves addressing and managing the aftermath of a security breach or attack, or incident. The structure of an intrusion (see the accompanying figure), in which an attacker gains and maintains access to an organization's networks tends to involve an attacker conducting reconnaissance to identify the system or network vulnerabilities, or services that can be

exploited to penetrate and maintain presence in the institution's network. Typically, following initial reconnaissance, the attacker will exploit the vulnerability to gain access or penetrate the host network. Once in, the attacker then aims to escalate privileges and/or move laterally to pivot from one machine to another, without raising alarms, in order to get access to the desired system. They are then often able to conduct exfiltration to steal critical assets while trying to maintain a persistent presence within the network to keep mining for new information (*continued below*).



The Structure of an Intrusion

To respond to an incident or compromise, the first priority is to identify the vulnerabilities exploited by the attacker, identify which systems or data sources have been exposed to the breach, and effectively recover these systems. Response usually involves five broad categories:

- **Identification** - The first step in an incident response investigation

is to identify users and systems that have been exposed to the threat. This can be done by comparing user activity or reviewing the event logs and alerts produced by systems and applications or monitoring the network traffic flowing in and out of the company to look for any signs of compromise.

- **Investigation** – The investigation involves identifying the vulnerabilities used by the attacker to infiltrate the network, identifying any data, IP, and user credentials that were exposed and/or exfiltrated, and trying to establish the attacker's intent. Time is of the essence, so it's critical to engage trained individuals who are well versed with the incident response readiness plan.
- **Containment** – The goal of containment is to limit damage and isolate the machines or network segments that were infected, and preserve the data to be analyzed. This usually involves short-term fixes to limit damage as soon as possible, such as isolating a network segment of infected workstations, or taking down production servers that were hacked and having all traffic routed to failover servers. Longer-term fixes involve preserving data on the infected machines to be analyzed later, and preparing to rebuild systems that were subjected to the attack. Under certain circumstances, the incident might be allowed to continue to gather evidence or identify the attacker.
- **Remediation** – This stage aims to validate that the compromised systems are wiped, reimaged and brought back into production, as well as confirming that there are no more signs of abnormality or malware on these systems including patching and updating the systems to enable stronger defense against similar future attacks.
- **Adaptation** – Learning from the event and creating a strong incident response readiness program, to ensure the firm will be able to handle future incidents. This includes documenting the incident and performing user awareness training.

- **Reactive Cybersecurity – Digital Forensics**

Digital forensics can be defined as, "The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal."[1] In other words, digital forensics is the practice of identification, collection, and analysis of artefacts present on a device which can be used to refute or support a hypothesis of data misappropriation, fraud or crime.

Although incident response and digital forensics leverage similar tools and resources, the fundamental difference is that the objective of an incident response review is to identify a quick and timely fix to the threat, whereas a digital forensic review usually involves an internal, regulatory or criminal investigation. Incident response is focused on containment of a prevailing threat, while digital forensic analysis is focused on understanding, remediating and reporting the findings of the incident.

Digital forensic matters can be broadly categorized into four categories:

- **IP Misappropriation** – Investigations involving theft of intellectual property for personal, economic or political gains or patent infringement litigations involving a comprehensive comparison of the source code to identify the commonality of the underlying algorithm.
- **Mobile Device Investigations** – with the increase in the number of smart phones and the amount of data these devices can store, mobile phone forensics is a rapidly growing avenue of investigation. Scrutiny may range from extraction of active communications for identifying the whereabouts of the user.
- **Hardware** – Cases where the suspect has attempted to destroy the device containing data relevant to the investigation or the data residing on the device isn't accessible using standard tools.

[1] DFRWS TECHNICAL REPORT - http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf We can find other definitions but I like the way this definition has been constructed and encompasses the important factors of digital forensic.

Involves removing the memory chip from the device and evaluating the disk at a sector level to extract data.

- **Data preservation, remediation, validation and recovery** – Cases in which the examiner has been tasked with preserving the data on electronic devices in a forensically sound manner to be compliant with a subpoena, litigation, or matters involving remediation of data from sources in a way that the removed data cannot be recovered. This includes recovering data that has been deleted.

A digital forensic investigation can broken-down into 4 broad phases

1. **Identification** – The goal is to identify users or systems that appear to act out of the norm and should be subjected to forensic review for evidence of fraud or crime in matters involving internal, regulatory or legal investigation.
2. **Collection/Imaging** – The process of creating a forensically sound copy of the data residing on a device to a media that can retain the data for extended period of time. *Forensically sound* means that the process used to create and store the image is acceptable by the law and provides assurance that the imaging methodology followed was the least intrusive method of maintaining the integrity of the device.
3. **Analysis** – The analysis phase involves identifying artefacts on the evidence which can be used to validate or refute the hypothesis of misconduct or crime. For instance, assessing the evidence to resolve queries like if and how a disgruntled ex-employee stole an organization's IP.
4. **Reporting** – The formal written account of facts and conclusions, after a thorough review of the evidence, presented in a number of formats, such as an affidavit, declaration, expert report, rebuttal, or report.

Conclusion

As the cyber risk spectrum changes, it is critical for an organization to understand and identify the security risks and potential threats that it needs to defend against. Cyber risk is no longer a concern only for organizations that hold sensitive or regulated data or intellectual property:

because of the convergence of the physical and digital worlds, cyberattacks can disrupt business operations and the ability to generate revenue. In order for an institution to confront and combat the multifaceted cyber threats, it is critical that it creates a proactive cybersecurity program, and be ready to respond when it is hit.

** Ashim Kapur is a Director in Stroz Friedberg's New York office where he assists with the management of the firm's technical operations in areas of computer forensics, electronic discovery, and incident handling. In addition to maintaining an active docket of cases and supervising forensic examiners, Mr. Kapur conducts digital forensic acquisitions and analyses of laptops, desktops, servers, phones, and tablets in civil litigations, criminal matters, internal investigations, and incident response efforts. Kapur assists in conducting and managing matters involving Anti Money Laundering and Compliance Technology Assurance services review.*

****

How Do we Compromise between Individual Desires and Societal Requirements?

Vincenzo Piuri

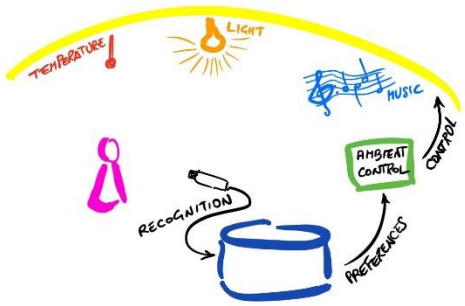
Ambient intelligence is a set of technologies that are pervasively embedded in the environment in which we live and work. They facilitate the human-system interaction and ensure the liveability by autonomously adjusting the environmental conditions. Instead of having humans themselves controlling the operating conditions of the environment (e.g., like in conventional domotics), ambient intelligence understands the needs and preferences of individuals and adds a layer of intelligence to the holistic operating conditions of the environment so that a direct human action on the control system ceases to be necessary.

Such a different perspective of an intelligently controlled ambiance will ensure a more comfortable and safer life, making the environment pre-emptively to understand the humans in it and not only to

receive passive commands and act on them. Opportunities for applying this principle come to us, every day: from domotics to assistance of elders as well as otherwise challenged or sick individuals, from entertainment to commerce and e-commerce, from health care to rental systems, from augmented reality to virtual and augmented tours, and much more.

Adaptability and advanced services for ambient intelligence require an intelligent technological support for understanding the current needs and desires of individuals in the environment, as well as for understanding the current status of the environment itself. This infrastructure constitutes an essential base for *smart* living.

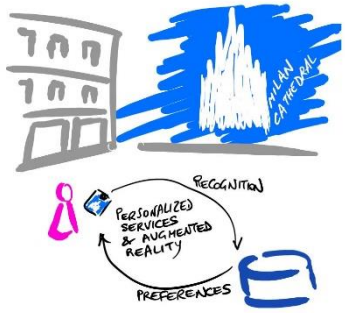
These days a multitude of technologies indeed happen to converge in support of creating efficient and effective infrastructures for ambient intelligence. Artificial intelligence can provide flexible techniques for designing, and for implementing and monitoring of control systems, that can be configured with data obtained from behavioral patterns or by mimicking approximate reasoning processes to achieve optimal adaptable systems. Machine learning can be effective in extracting knowledge from data and learn the actual and desired behaviors and needs of individuals as well as the environment to form informed decisions in managing the environment itself and, furthermore, its adaptation to the people's needs. Biometrics can help in identifying individuals or groups: their profiles can be used for adjusting the behavior of the environment. Machine learning can be exploited to dynamically learn the preferences and needs of individuals and enrich/update the profile associated either to such individual or a group. Biometrics can further be used to create advanced human-computer interaction frameworks. Cloud computing and Internet-of-Things will be instrumental in encouraging world-wide availability of knowledge about the preferences and needs of individuals as well as services for ambient intelligence on which applications may be easily developed. It is obviously important to note that security and privacy are critical aspects for ensuring user acceptance and actual usability of the entire infrastructure.



The holistic integration of these various technologies will provide the comprehensive infrastructure in supporting adaptable operations and intelligent services for smart living in ambient intelligent infrastructures.

On the flip side, a pervasive approach like the one depicted above has many critical aspects concerning people interaction, sociology, psychology, privacy, ethics, and social implications of technologies. Access to personal needs, preferences and desires, in particular, constitutes a very sensitive information which should be protected: each individual should be able to control the disclosure of such information to individual applications so as to make conscious decisions about visibility of the subject's inclinations and prevent its misuse and drawing inappropriate inferences. Presence of people in an environment implies a definition of collective strategies for

choosing the operating conditions of the environment by considering the multifarious needs and preferences of each of them, and then dynamically cater to the collective needs of the human groups living in the same environment. Ethical aspects related to proper use of knowledge extracted from individual needs and preferences are also significant: knowledge should be used to support people within the specific goals and environments for which information has been disclosed to the environment management system, without inferring anything related to personal behavior and without disclosing information as to how it was obtained and about location and movements of individuals. These aspects are particularly critical with respect to marketing activities, commercial targeting purposes, or government monitoring. The use of ambient intelligence should always be at the service of the people and not be used to control or limit them and their freedom of thinking, expression, and lawful behavior.



****

This month's notable presentation

IEEE PES Power & Energy Society™

POWER & ENERGY SOCIETY
INDUSTRY APPLICATIONS SOCIETY
LIFE MEMBERS AFFINITY GROUP
NEW YORK SECTION

IAS

You are invited to a meeting of the PES & IAS NY Chapter and the NY LMAG on:

Emergency Standby Power Systems using Paralleling Switchgear - Automatic Transfer Switches - Circuit Breakers

Tuesday, July 24th, 2018

THE PRESENTATION:

Tonight's program is a consecutive presentation of two related courses. Course 1 reviews the basics of an **On-site Emergency Standby Power System** consisting of engine generators and paralleling controls where Automatic Transfer Switches are used to transfer between utility and generator sources. This course will include a basic review of Automatic Transfer Switch types and configurations, and the basic functions of paralleling controls. This relates mostly to standardized generator set-mounted paralleling systems. Course 2 reviews the **Basics of "Traditional" Paralleling Systems** where Circuit Breakers are used to transfer between utility and generator sources. This course will review the design sequence for custom-built paralleling switchgear, the nine (9) common configurations, the sequence of operation, as well as documentation and programming.

THE SPEAKER: William Howard, Sales Manager – Engineered Systems, KOHLER Power Systems:

William Howard is Sales Manager – Engineered Systems for KOHLER Power Systems (Kohler, Wisconsin), one of a nationwide, locally-deployed staff of direct factory employees, providing product and engineering support relating to KOHLER Power Systems products and systems, to Design Professionals as well as Distributor salespeople and staff. Bill is a NYC-area native who has served in the emergency standby power marketplace since 1988, mostly within the KOHLER world (with Cooper Power Systems, the local KOHLER Distributor), with several side trips into the wider distributed power generation (CHP, CCHP) industry, prior to joining KOHLER in 2012. Bill earned his B.S. in Mechanical Engineering from Cornell University.