International Council For Industrial Security & Safety Management

ICISS

Newsletter: June 2016

Let's professionalize the professionals…

The time has come for another paradigm shift in the field of Industrial security in India and likewise in many other countries. After the PSAR Act 2005, there was expectation of standardizing this sector and establishing the bench marks. The thought leaders of the industry had and rightly so, talked of emerging fields of partnership with governmental law-enforcing agencies and private security service providers. It was believed that soon there will be scene in which police will be withdrawing from the duties of social policing and security of public places. It was believed that airports, seaports and other transport hubs can be and will be policed by the private security personal and police will have all time, energy and resources for crime investigation and maintaining law-and-order.

To succeed in this direction first and foremost need is to empower the police and then make necessary information available to those private security officials who will need them for official discharge of their duties. The needed information may sometimes be even classified but nature of the duties to be entrusted to private security will need them to be shared. For example those engaged in immigration or narcotics control may need criminals' data base which is classified information but essential for those who are involved in such responsibilities but are from private security agencies. To handle such issues a nodal authority in needed.

In this direction, many countries working towards Private Public Partnership model in security management and Policing need to examine and study American approach for suitable changes at their level.

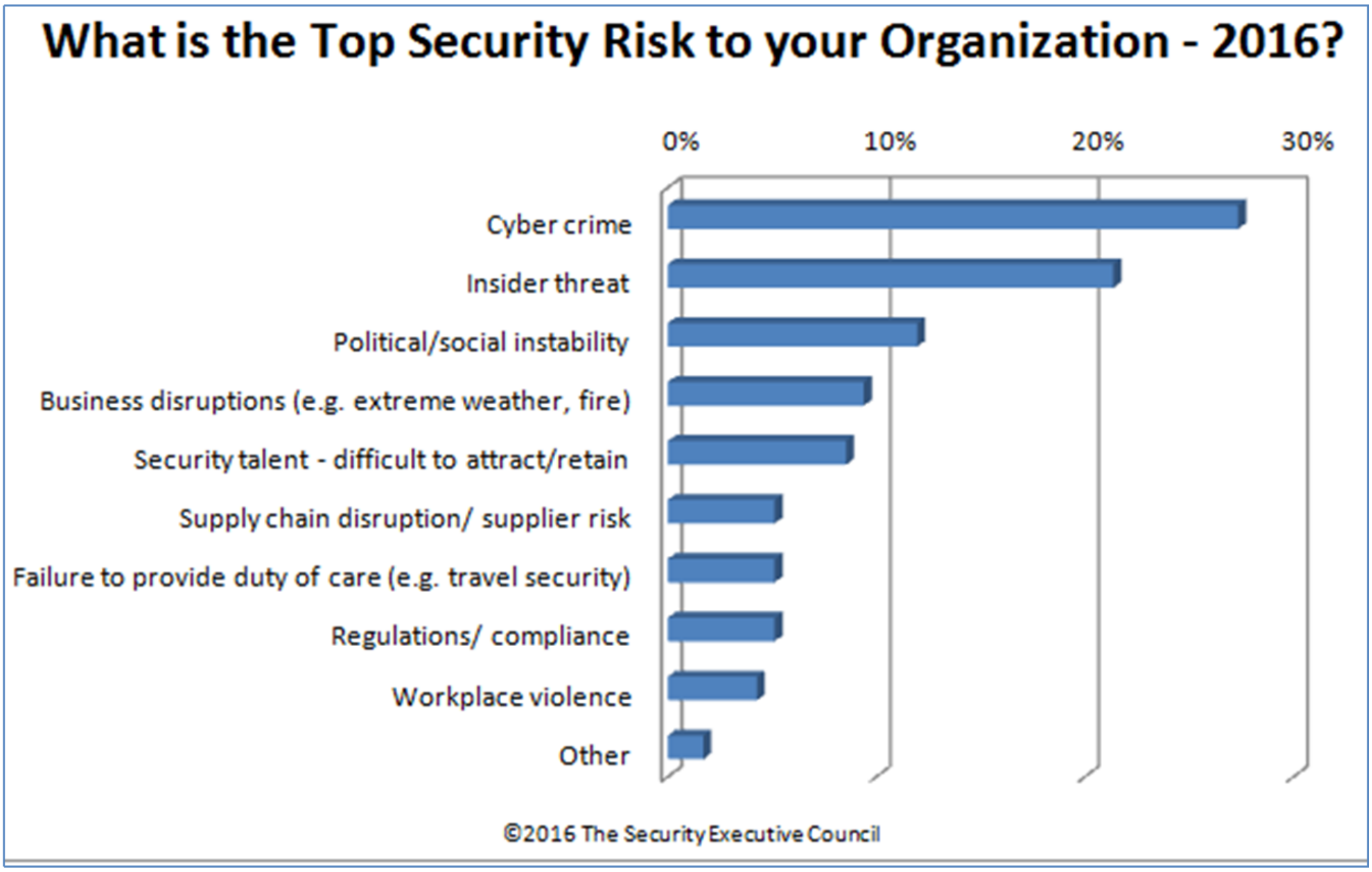
The National Industrial Security Program, or NISP, is the nominal authority (in the United States) for managing the needs of private industry to access classified information. The NISP was established in 1993 by Executive Order 12829. The National Security Council nominally sets policy for the NISP, while the Director of the Information Security Oversight Office is nominally the authority for implementation. Under the ISOO, the Secretary of Defence is nominally the Executive Agent, but the NISP recognizes four different Cognizant Security Agencies, all of which have equal authority: the Department of Defence, the Department of Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission

Capt S B Tyagi
For ICISS

ICISS International Council For Industrial Security And Safety Management

Top Security Risk to Organizations Today - 2016

The Security Risks Landscape Continues to Evolve! Over the past decade we have experienced significant changes in the security and risk mitigation field. As organizations become leaner and more agile the mitigation of security risks becomes more important than ever in protecting the organization's assets and people. It is becoming imperative that all business functions maintain focus on the tasks that really matter to the organization.

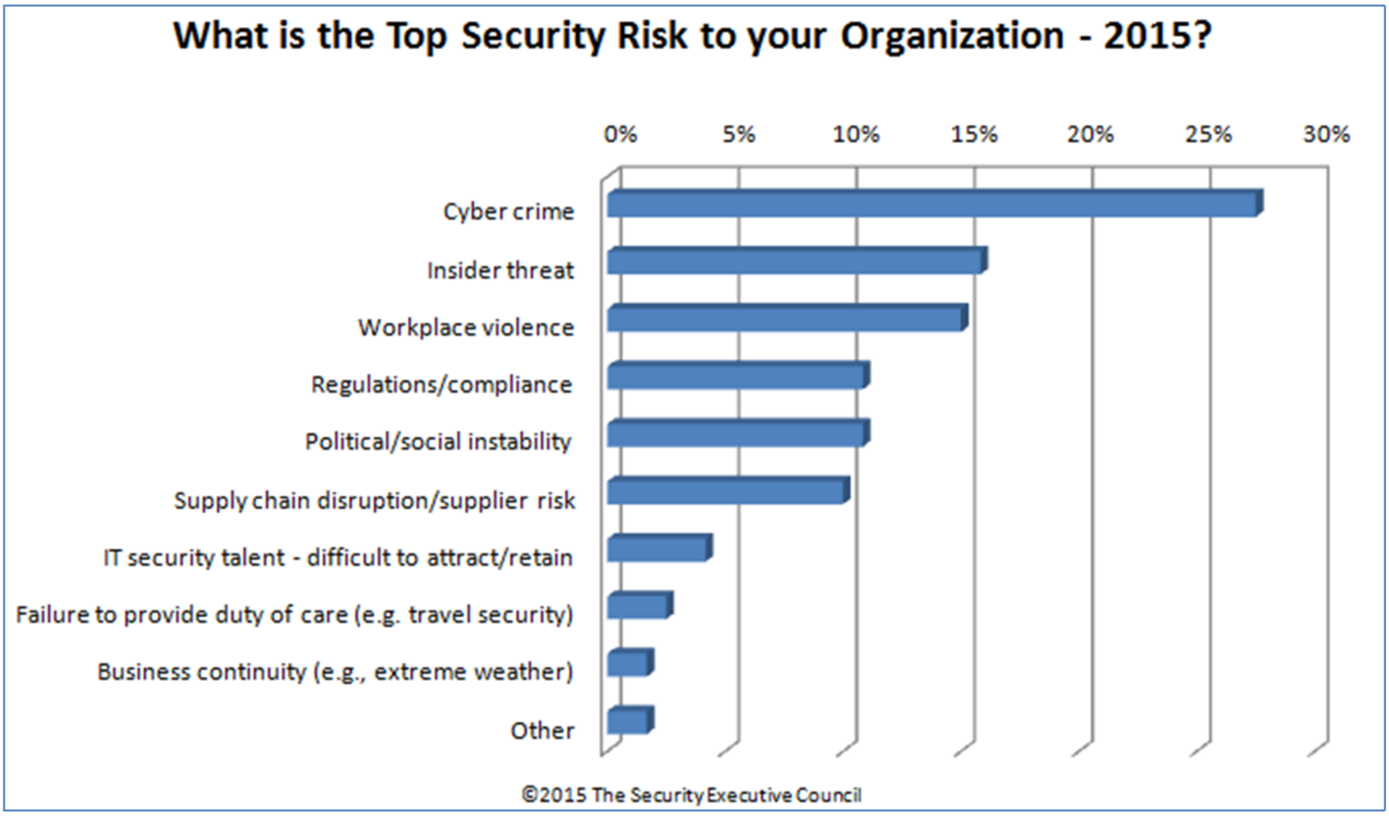


Each organization has a different take on what is important. This security barometer is investigating what issues security risk mitigation executives are focusing on today. Every organization faces unique challenges. The industry as well as the culture of the organization work to define the perspectives of the risk management personnel working within that particular environment. This means that there is no right or wrong answer to the question "what is the top security risk to your organization today?"

Instead, our goal is to help identify trends and provide you information to consider and compare to what you are seeing within your organization.

Top Risks as Reported in 2015

We have been asking for your opinion regarding top risks since 2010. You can compare the results from this latest poll to the results from 2015 shown below.



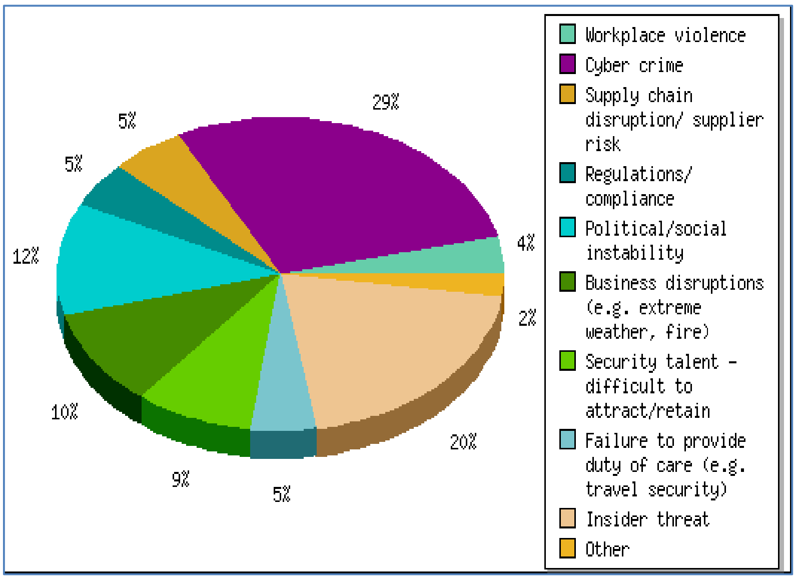
©2015 The Security Executive Council

The Top Security Risks Facing Organizations Today - 2016

Every organization faces their own unique challenges. Here are what your peers report as the top security risk to their organization today.

How businesses are tackling security issues

Industries follow best practices and best solutions available in the market, to stay ahead of the new threats. However, threats seek the loopholes including the weakest links in the network or physical security set-up. Following are some of the emerging security trends and business priorities for 2016.



1. Organizations adopting a more comprehensive approach to physical and digital risk management
2. Organizations increasingly acquire new security skills, vendor products and services to embrace an adaptive security architecture for protection from advanced threats.
3. Regulators becoming increasingly aware of data security compliance, data export controls and privacy laws enforcement.

4. IoT acceleration that converges information technology and operational technology security, blurring the line between the physical and digital world.

https://www.securityexecutivecouncil.com/secbar/results.html?sid=95365

Business-security Risks and How You can Fight-back?

Security breaches again made big news in 2014. Yet despite years of headline stories about security leaks and distributed denial-of-service (DDoS) attacks and repeated admonishments from security professionals that businesses (and individuals) needed to do a better job protecting sensitive data, many businesses are still unprepared or not properly protected from a variety of security threats.

Indeed, according to Trustwave's recent 2014 State of Risk Report, which surveyed 476 IT professionals about security weaknesses, a majority of businesses had no or only a partial system in place for controlling and tracking sensitive data.

So, what can companies do to better protect themselves and their customers', sensitive data from security threats? CIO.com queried dozens of security and IT experts to find out. Following are the six most likely sources, or causes, of security breaches and what businesses can, and should, do to protect against them.

Risk No. 1: Disgruntled Employees

"Internal attacks are one of the biggest threats facing your data and systems," states Cortney Thompson, CTO of Green House Data. "Rogue employees, especially members of the IT team with knowledge of and access to networks, data centers and admin accounts, can cause serious damage," he says. Indeed, "there [were] rumors that the Sony hack was not [carried out by] North Korea but [was actually] an inside job.

[Related: Sony Hack Is a Corporate Cyberwar Game Changer]

Solution: "The first step in mitigating the risk of privileged account exploitation is to identify all privileged accounts and credentials [and] immediately terminate those that are no longer in use or are connected to employees that are no longer at the company," says Adam Bosnian, executive vice president, CyberArk.

[Related: When Rogue IT Staffers Attack: 8 Organizations That Got Burned]

"Next, closely monitor, control and manage privileged credentials to prevent exploitation. Finally, companies should implement necessary protocols and infrastructure to track, log and record privileged account activity [and create alerts, to] allow for a quick response to malicious activity and mitigate potential damage early in the attack cycle."

Risk No. 2: Careless or Uninformed Employees

"A careless worker who forgets [his] unlocked iPhone in a taxi is as dangerous as a disgruntled user who maliciously leaks information to a competitor," says Ray Potter, CEO, SafeLogic. Similarly, employees who are not trained in security best practices and have weak passwords, visit unauthorized websites and/or click on links in suspicious emails or open email attachments pose an enormous security threat to their employers' systems and data.

Solution: “Train employees on cyber security best practices and offer ongoing support,” says Bill Carey, vice presdient of Marketing for RoboForm. “Some employees may not know how to protect themselves online, which can put your business data at risk,” he explains. So it's essential to “hold training sessions to help employees learn how to manage passwords and avoid hacking through criminal activity like phishing and keylogger scams. Then provide ongoing support to make sure employees have the resources they need.”

Also, “make sure employees use strong passwords on all devices,” he adds. “Passwords are the first line of defense, so make sure employees use passwords that have upper and lowercase letters, numbers and symbols,” Carey explains.

“It's also important to use a separate password for each registered site and to change it every 30 to 60 days,” he continues. “A password management system can help by automating this process and eliminating the need for staff to remember multiple passwords.” Encryption is also essential.

“As long as you have deployed validated encryption as part of your security strategy, there is hope,” says Potter. “Even if the employee hasn't taken personal precautions to lock their phone, your IT department can execute a selective wipe by revoking the decryption keys specifically used for the company data.”

To be extra safe, “implement multifactor authentication such as One Time Password (OTP), RFID, smart card, fingerprint reader or retina scanning [to help ensure] that users are in fact who you believe they are,” adds Rod Simmons, product group manager, BeyondTrust. “This helps mitigate the risk of a breach should a password be compromised.”

Risk No. 3: Mobile Devices (BYOD)

“Data theft is at high vulnerability when employees are using mobile devices [particularly their own] to share data, access company information, or neglect to change mobile passwords,” explains Jason Cook,CTO & vice president of Security, BT Americas. “According to a BT study, mobile security breaches have affected more than two-thirds (68 percent) of global organizations in the last 12 months.”

Indeed, “as more enterprises embrace BYOD, they face risk exposure from those devices on the corporate network (behind the firewall, including via the VPN) in the event an app installs malware or other Trojan software that can access the device's network connection,” says Ari Weil, vice president, Product Marketing, Yottaa.

[Related: 2015 Mobile Security Survival Guide]

Solution: Make sure you have a carefully spelled out BYOD policy. “With a BYOD policy in place, employees are better educated on device expectations and companies can better monitor email and documents that are being downloaded to company or employee-owned devices,” says Piero DePaoli, senior director, Global Product Marketing, Symantec. “Monitoring effectively will provide companies with visibility into their mobile data loss risk, and will enable them to quickly pinpoint exposures if mobile devices are lost or stolen.”

[Related: How to Create Seamless Mobile Security for Employees]

Similarly, companies should “implement mobile security solutions that protect both corporate data and access to corporate systems while also respecting user’s privacy through containerization,” advises Nicko van Someren, CTO, Good Technology. “By securely separating business applications and business data on users’ devices, containerization ensures corporate content, credentials and configurations stay encrypted and under IT’s control, adding a strong layer of defense to once vulnerable a points of entry.”

You can also “mitigate BYOD risks with a hybrid cloud,” adds Matthew Dornquast, CEO and cofounder, Code42. “As unsanctioned consumer apps and devices continue to creep into the workplace, IT should look to hybrid and private clouds for mitigating potential risks brought on by this workplace trend,” he says. “Both options generally offer the capacity and elasticity of the public cloud to manage the plethora of devices and data, but with added security and privacy—such as the ability to keep encryption keys on-site no matter where the data is stored—for managing apps and devices across the enterprise.”

Risk No. 4: Cloud Applications

Solution: “The best defense [against a cloud-based threat] is to defend at the data level using strong encryption, such as AES 256-bit, recognized by experts as the crypto gold standard and retain the keys exclusively to prevent any third party from accessing the data even if it resides on a public cloud,” says Pravin Kothari, founder and CEO of CipherCloud. “As many of 2014’s breaches indicate, not enough companies are using data level cloud encryption to protect sensitive information.”

> **"The second most important need after food and shelter is the need for protection and security. That comes even before the need for love, social esteem and self-growth. Believe it or not; ask yourself and you'll know it's true."**
>
> **Abraham Maslow, a renowned psychologist**

Risk No. 5: Unpatched or Unpatchable Devices

“These are network devices, such as routers, [servers] and printers that employ software or firmware in their operation, yet either a patch for a vulnerability in them was not yet created or sent, or their hardware was not designed to enable them to be updated following the discovery of vulnerabilities,” says Shlomi Boutnaru, cofounder & CTO, CyActive. “This leaves an exploitable device in your network, waiting for attackers to use it to gain access to your data.

[Related: Are You Ready for the End of Windows Server 2003]

“On July 14, 2015, Microsoft will no longer provide support for Windows Server 2003 – meaning organizations will no longer receive patches or security updates for this software,” notes Laura Iwan, senior vice president of Programs, Center for Internet Security.

With over 10 million physical Windows 2003 servers still in use, and millions more in virtual use, according to Forrester, “expect these outdated servers to become a prime target for anyone interested in penetrating the networks where these vulnerable servers reside,” she says.

Solution: Institute a patch management program to ensure that devices, and software, are kept up to date at all times. “Step one is to deploy vulnerability management technology to look on your network and see what is, and isn't, up to date,” says Greg Kushto, director of the Security Practice at Force 3. “The real key, however, is to have a policy in place where everyone agrees that if a certain piece of equipment is not updated or patched within a certain amount of time, it is taken offline.”

To avoid potential problems re Windows Server 2003, “identify all Windows Server 2003 instances; inventory all the software and functions of each server; prioritize each system based on risk and criticality; and map out a migration strategy and then execute it,” Iwan advises. And if you are unable to execute all steps in house, hire someone certified to assist you.

Risk No. 6: Third-party Service Providers

“As technology becomes more specialized and complex, companies are relying more on outsourcers and vendors to support and maintain systems,” notes Matt Dircks, CEO, Bomgar. “For example, restaurant franchisees often outsource the maintenance and management of their point-of-sale (POS) systems to a third-party service provider.”

However, “these third-parties typically use remote access tools to connect to the company’s network, but don’t always follow security best practices,” he says. “For example, they’ll use the same default password to remotely connect to all of their clients. If a hacker guesses that password, he immediately has a foothold into all of those clients’ networks.”

Indeed, “many of the high profile and extremely expensive breaches of the past year (think Home Depot, Target, etc.) were due to contractor’s login credentials being stolen,” states Matt Zanderigo, Product Marketing Manager, ObserveIT. “According to some recent reports, the majority of data breaches – 76 percent – are attributed to the exploitation of remote vendor access channels,” he says. “Even contractors with no malicious intent could potentially damage your systems or leave you open to attack.”

“This threat is multiplied exponentially due to the lack of vetting done by companies before allowing third parties to access their network,” adds Adam Roth, cybersecurity specialist from Dynamic Solutions International. “A potential data breach typically does not directly attack the most valuable server, but is more a game of leap frog, going from a low level computer that is less secure, then pivoting to other devices and gaining privileges,” he explains.

“Companies do a fairly good job ensuring critical servers avoid malware from the Internet,” he continues. “But most companies are pretty horrible at keeping these systems segmented from other systems that are much easier to compromise.”

Companies need to validate that any third party follows remote access security best practices, such as enforcing multifactor authentication, requiring unique credentials for each user, setting least-privilege permissions and capturing a comprehensive audit trail of all remote access activity. In particular, “disable third-party accounts as soon as they are no longer needed; monitor failed login attempts; and have a red flag alerting you to an attack sent right away,” says Roth.

General Guidance on Dealing With Breaches

“Most organizations now realize that a breach is not a matter of if but when,” says Rob Sadowski, director of Technology Solutions for RSA. To minimize the impact of a security breach and leak, conduct a risk assessment to identify where your valuable data resides and what controls or procedures are in place to protect it. Then, “build out a comprehensive incident response [and disaster recovery/business continuity] plan, determining who will be involved, from IT, to legal, to PR, to executive management, and test it.”

Courtesy: Jennifer Lonoff Schiff

Top 10 cyber security threats for Oil and Gas industry

With the exploitation of new cost-effective operational concepts, use of digital technologies and increased dependence on cyber structures, the oil and gas industry is exposed to new sets of vulnerabilities and threats, DNV GL writes in an article identifying the biggest cyber security threats to the oil and gas industry. According to the company, cyber-attacks have grown in stature and sophistication, making them more difficult to detect and defend against, and costing companies increasing sums of money to recover from.

DNV GL is today delivering a cybersecurity study to the Lysne Committee, a body appointed by the Norwegian Ministry of Justice and Public Security to assess the country’s digital vulnerabilities. DNV GL’s study reveals the top ten most pressing cyber security vulnerabilities for companies operating offshore Norway.

An international DNV GL survey of 1,100 business professionals found that, although companies are actively managing their information security, just over half (58%) have adopted an ad hoc management strategy, with only 27% setting concrete goals, the company has said.

“Headline cyber security incidents are rare, but a lot of lesser attacks go undetected or unreported as many organizations do not know that someone has broken into their systems. The first line of attack is often the office environment of an oil and gas company, working through to the production network and process control and safety systems," says Petter Myrvang, head of the Security and Information Risk, DNV GL – Oil & Gas.

DNV GL says that while the study focused on operations on the Norwegian Continental Shelf, the issues are equally applicable to oil and gas operations anywhere in the world.

The top ten cyber security vulnerabilities:

1. Lack of cyber security awareness and training among employees
2. Remote work during operations and maintenance
3. Using standard IT products with known vulnerabilities in the production environment
4. A limited cyber security culture among vendors, suppliers and contractors
5. Insufficient separation of data networks
6. The use of mobile devices and storage units including smartphones
7. Data networks between on- and offshore facilities
8. Insufficient physical security of data rooms, cabinets, etc.
9. Vulnerable software
10. Outdated and ageing control systems in facilities

DNV GL has said it believes cyber security vulnerabilities can be addressed through a risk-based approach, using the bow-tie model familiar in safety barrier management. This allows companies to identify the threats to and vulnerabilities of assets and operations and plan barriers to prevent incidents and mitigate the consequences of cyber risks. This includes procedures to maintain the barrier quality documented in performance standards.

"As all oil and gas process plants are now connected to the Internet in some way, protecting vital digital infrastructure against cyber-attacks also ensures safe operations and optimal production regularity," says Trond Winther, head of the Operations Department, DNV GL – Oil & Gas.

BASIS 2016: Smart Security – The Doors to the Future

Capt SB Tyagi, Chief Councillor of ICISSM made a key-note presentation on the subject of "Global Threats to Oil & Gas Installations" during the event.

BASiS 2016
Building A Secure India Summit
Smart Security
the doors to the future
May 20, 2016 | Double Tree by Hilton, Gurgaon
Supporting Partner
ICISS
International Council For Industrial Security And Safety Management
Keynote Partner
HID
Silver Partner
APS GROUP
Roundtable Partner
ORION SECURE
ORION SECURITY SOLUTIONS PRIVATE LIMITED

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

Suggestions & feedback may be sent to us on e-mail: onlineicissm@gmail.com

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!