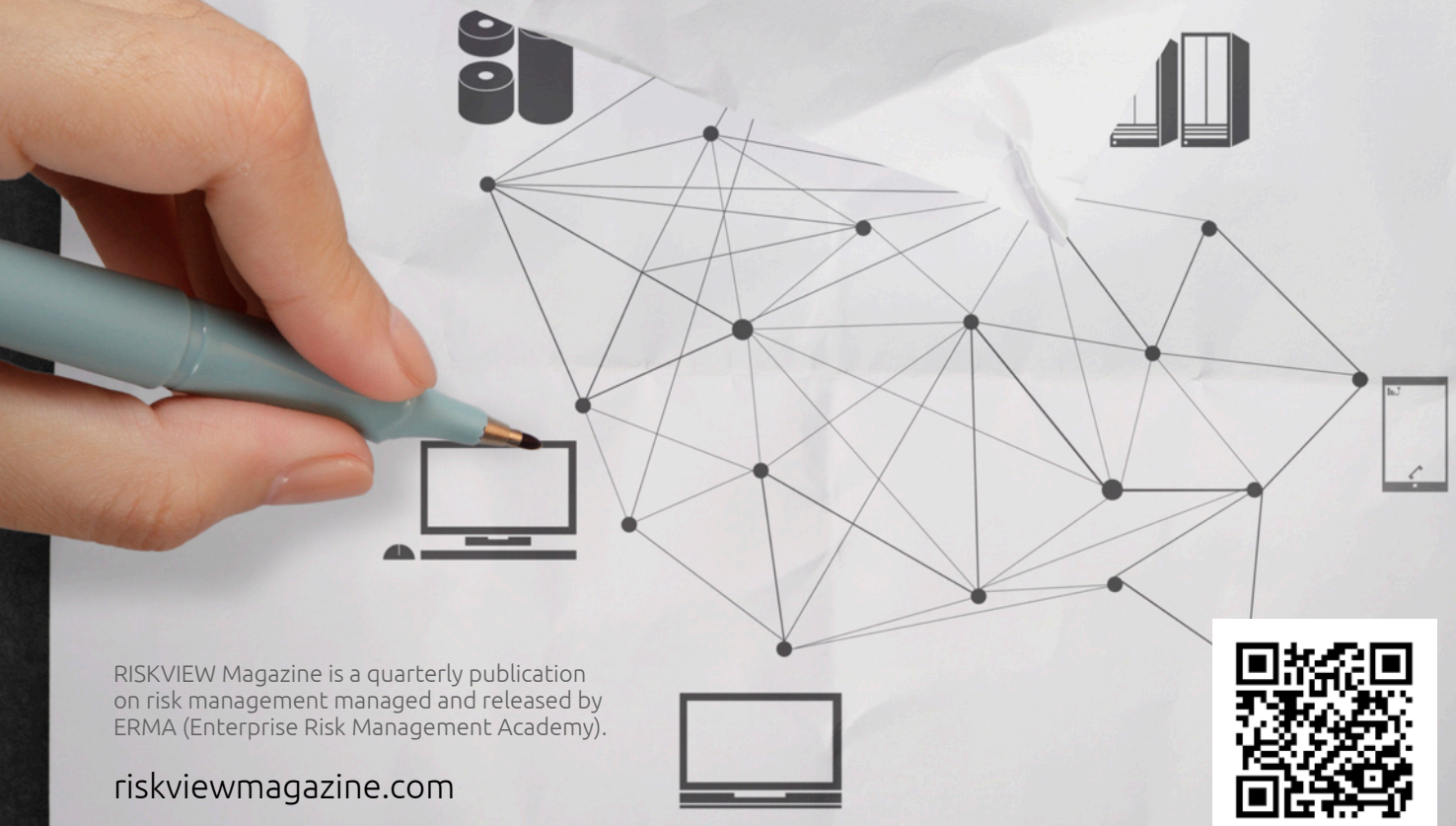
ERMA | ENTERPRISE RISK MANAGEMENT ACADEMY

RISKVIEW

RISKVIEW MAGAZINE #1 | MARCH 2015

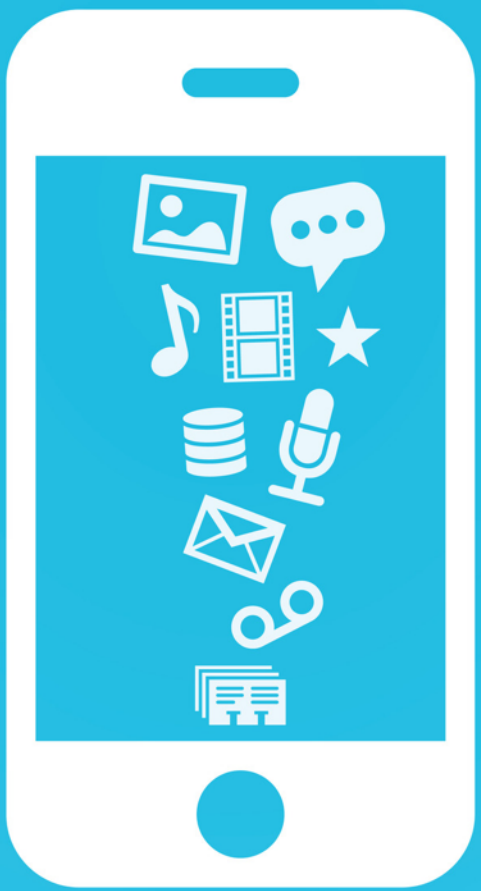
THE MANY SIDES OF CYBER RISK



RISKVIEW Magazine is a quarterly publication on risk management managed and released by ERMA (Enterprise Risk Management Academy).

riskviewmagazine.com

FACING CYBER RISK



Cloud and mobile devices are no longer strangers for individuals and organizations. The so-called modern life is even built surrounding these cloud services.

We all know that new and exciting opportunities and threats lie in this cyber age, but how far do we understand the threats that came along with all of these technology advancements?

This very first edition of RiskView Magazine, published by ERMA, Enterprise Risk Management Academy, will try to answer this question by featuring several article on cyber risk from different angles.

Happy reading!

IN THIS EDITION

RISK MANAGEMENT AND DATA ANALYTICS

Not many people understand that data analytics is important in risk management control and strategy. People who don't have business background won't understand that the right data can improve a company in the maximum way, while the wrong data can send everything in spirals and chaos. In today's global platform, where everything relies so much on data, it is crucial that data analytics and management can be put forward and sorted out efficiently.

If you have been around in this industry, you understand that data isn't only important to help your business grow, but also to deal with the increasing competitive atmosphere. That's why more techniques and technologies to analyze and manage data can deliver far more effective and efficient outcome.

First of all, the right data can lead you to making decisions of what to do with your important information – which can lead to better cyber security and protection, as well as the preventive methods of how to deal with the possible threats.

Second, the data you have can lead you to create smarter and more creative ways in mitigation strategies as well as better business strategies.

Third, the data can help you improve your business in the most efficient ways, without you having to worry about greater risks as everything has been minimized and planned out carefully.

It is crucial that data analytics and management can be put forward and sorted out efficiently.

Risk Management.
VISUALIZED.
The latest risk management insight in the form of infographics.

visit erm-academy.org

However, the problem with today's data is how fast they come and go, and how abundant they are. If you have a business of your own, you know that data is coming from different directions; all coming and creating crowded environment. It is a good thing that the hardware cost to store the data has decreased, so the cost for operation won't be overwhelming. But still, with so many data flying around, someone has to be responsible for analyzing and managing it. Someone has to sort out different data; separating the important data from the useless one. You will be surprised of how irrelevant and useless data can create distraction and damage when not managed properly. If you want your business to succeed, you certainly only want to use relevant and helpful data that can support your operation; that's why effective analytic program and data management is vital to deal with data flood and abundance.

"You will be surprised of how irrelevant and useless data can create distraction and damage when not managed properly."

Moreover, coming up with relevant and the right data will lead to solid and sound actionable information, which is absolutely important for the run of the business.

That's why synthesizing and analyzing the right data shouldn't be underestimated or taken up lightly. Those who are responsible for sorting out the data hold very important role in the success of the business itself. It is a good thing that new techniques and tools to deal with large numbers of data have been found, created, and developed. In fact, new tools have been progressing from time to time, whether you deal with specific small platform or with the entire community and ecosystem. A professional and skilled analyst should be able to make professional process and decisions of how to manage the data flood and sort everything through. Their job includes presenting the right data to the right decision maker at the right time and place, limiting technical details while focusing and enhancing the important information for actionable results. The information they relay should be understandable, timely, correct, and sufficient.

It is safe to say that business should focus on their data if they want to develop, flourish, and succeed. They should collect, store, manage, and analyze the data in the most efficient ways to help the business run efficiently and effectively. Professional analyst should also be included within the platform; not only they will be handy for the company, but they will also provide solid risk management system that is safe and reliable.

THE BENEFITS OF BIG DATA

Many sectors are using Big Data to be effective and efficient. These are the top five sectors that Big Data has been involved with:

SECURITY

National organizations such as GCHQ and NSA are known to heavily use Big Data as their law enforcement. Big Data assists them to provide unlimited data to solve criminal cases, terrorist plots, and public security issue.

HEALTH

Big Data is able to speed up the researchers work by its analytics system. For instance, it can help to decode DNA strings just in minutes to help researchers' work in finding the cures and predicting the patterns of diseases. Big Data can also monitor premature and sick babies by analyzing the heart beats and breathing patterns. Faster analysis results can lead to more saved lives.

SCIENCE

Big Data takes part in space exploration since it needs a full capacity data provider 100 times stronger than the Internet. Amazon and NASA are also using Big Data as their radar to seek for another life on another planet.

RETAIL

Big Data has major roles in improving retailers' income. Big Data analysis takes part in improving inventory management by planning their selling strategy and helping the companies such as Amazon and Netflix in producing recommendation engines.

FINANCE

High Frequency Trading uses Big Data algorithms to produce trading decisions. Big Data is also reporting all of the pre-trade communications data to keep track on financial organizations.

MAKING EMPLOYEES UNDERSTAND ABOUT DATA RISK

When there is a case of stolen confidential information, it will harm the state of the businesses. It is no wonder that the case is considered as one of the crucial risks for business owners.

To handle this kind of risk, IT department plays an important role as electronic data protector. However, there are also other sensitive data of the customers and employees in the form of files that are in need of the same protection, such as credit card information, Social Security numbers, etc. If you fail to protect them, it will only lead to another case of identify fraud or theft. The worst scenario is your customers won't trust you anymore and you have to get ready when they want to file a lawsuit.

Employees who are violating IT security policies and exposing the company network to unwanted risks are the cause of data loss in companies. Based on a survey of the first annual ISACA IT Risk/ Reward Barometer, there are top three reasons why employees can be the cause of risks for businesses and IT. 50% participants in the survey thought that employees are not protecting confidential data in accordance to the companies' standard, while 33% correspondents said that they do not fully comprehend the IT policies. In addition, there are 32% participants who believe that employees are using online services and non-approved software to do their work. Through the study, it is shown how employees take an important part when it comes to IT security.

> The worst scenario is your customers won't trust you anymore and you have to get ready when they want to file a lawsuit

As business owners, you have to make sure that your employees follow every step to protect any kinds of confidential data. It is suggested for you to provide your employees a secure cabinet or drawer to lock up the important files. Do not let your employees leave important information on their desk without guarding them. When your employees need to leave their desk, make sure that the files are safe in a secure place. In addition, when they use their personal devices to work, you need to educate them how to secure the devices properly.

Moreover, your employees also need to be aware of your company network security. Inform them how viruses, spyware, and other malicious contents are able to invade your confidential data in few seconds. When employees deal with electronic security, ask them to create strong and sophisticated passwords and assist them in recalling the passwords so they won't write them down on a piece of paper.

Remind your employees to be wary of any kinds of suspicious emails with attachment. If it is possible, provide them the list of dangerous file name extensions. You also need to educate them on the effects of installing unauthorized software on their computers to the company networks. Do not forget to block any kind of sites that are not related to your employees' jobs since there is a possibility that your network can be infected by malicious contents through wrong websites.

When you educate your employees with necessary information regarding your network security and urge them to protect it, the safety of your network can be guaranteed. However, if your employees do not understand the importance of data security in your company, it will lead to the crucial risk that can harm your company. Thus, the more knowledgeable your employees are about the data security, the more they understand their role in protecting your company.

DISCOVER. EXPLOIT. OPTIMIZE.

NEW POSSIBILITIES

ENTERPRISE RISK MANAGEMENT

CERTIFIED PROFESSIONAL

ERMCP or Enterprise Risk Management Certified Professional is a professional certification issued by ERMA, designed on the ground of ISO 31000 Risk Management International Standard.

ERMCP is given to professionals who are well experienced in the field of enterprise risk management and can demonstrate their knowledge, experiences and skills in managing the ERM process, which consists of at least the following processes: setting the context, identifying risk, assessing risk, mitigating risk, and monitoring it.

ERMCP
Enterprise Risk Management
CERTIFIED PROFESSIONAL
ERM ACADEMY

Visit **erm-academy.org/ermcp**

A BETTER CYBER SECURITY

The result of the 2014 Cost of Data Breach Study conducted by the Ponemon Institute for IBM revealed the stolen record of U.S business containing customer information is $201 on average.

Mostly the accident is caused by malicious attack instead of process failure and human error. In 2013, the data of mega-retailer Target had been hacked and they had to pay cash to lessen the damage, not to mention how the attack affected more than 110 million customers. On the other hand, similar case can lead a company to destruction. That explains how risky data breaches are for companies around the globe.

In this case, it is important for you to improve or strengthen your cyber security. However, what actions are you going to take to improve your cyber security? Fortunately, Ken Ammon, chief strategy officer at Xceedium Inc which is based in Herndon, Virginia, gives you meaningful advice regarding the matter:

Being Critical

Being critical here means you have to ask more questions and take a closer look at your chosen suppliers. You have to set boundaries between your suppliers and your company's system. The data breach in Target seemingly came through an HVAC contractor. To avoid walking on the same path, it is important for you to be critical when you face your suppliers. It would be better if your system is able to separate the users based on their roles. Platforms can be used to make your authentication system stronger by adopting two – factor authentications and a single sign – on. You can easily access them through your IT providers.

Knowing how hackers work

Is hacker from the inside of company more dangerous instead of the outside one? Both types of hackers are dangerous for the state of any companies. Outside hackers tend to use LinkedIn to look for your administrators and what kind of system they use. After that, they send a spear phishing email to steal their confidential information. In addition, hackers from the inside know how the system works. When they see that your security defense is weak, they will not hesitate to steal the data as long as there is a chance.

When dealing with cyber attacks, you have to think thoroughly what actions you should take to cover the damage since your actions will determine the future of your business.

Establishing security policy

Security policy is essential to protect your company. If you allow your employees to connect their personal devices on your network system, you have to make sure that the system is protected before the employees have access on it. Stating what is allowed and disallowed in your policy clearly, including consequences when violating them, so your employees won't cross the line. If necessary, train your network users regarding cyber security to reduce the risk. You are also suggested to use cloud-based service to deliver office automation support platforms if they offer two – authentication support to be used by administrators

Keep tabs on the security

When you cooperate with a larger company, you need to assure them that you are aware of how important the security system is. Thus, you need to acknowledge what matters on security by setting boundaries and observing employees. You can set password orientation for administrators and use two – factor authentications. Those two steps will enable you to secure the system.

.

HOW TO MANAGE **DIGITAL VOICES** WISELY?

In these modern times, corporate need to learn how to embrace the principle of digital voices and how to use it for the company's benefits. With so many people using digital media nowadays, the lines between facts and opinions become blurry; you cannot really tell which one is the truth and which is opinion based only.

The social media has its own perks and benefits, and yet there are some flaws that you need to consider about. Of course, you are free to say whatever you have in mind, influencing others as you go along your way. But this freedom is also the downside as you cannot really filter what you are about to say; let alone to really think about it and how it will affect others. Stating your opinions is truly easy. All you have to do is write whatever comes in mind and press on the 'send' button to make it go viral. However, once you press that button, things will never be the same anymore.

This is only a simple example of how digital voice affects your own personal life; imagine the scope when it is about a company – their work, their performance, and their products? That is why corporate needs to learn about these things when they want to have better risk management system – for their names and their credibility.

- Do embrace social media, but be transparent about it and don't go overboard.
- When making reviews, think carefully about the impacts to others – other companies, their performance, etc.
- Develop a new corporate culture where you can get objective ideas and voices.
- Look into your own corporate – especially your employees. They are your biggest assists when it comes to social change, passion, innovation, culture, and pride.
- Don't forget that reputation should always be included in your risk management planning. It is, after all, the important tool of your success.

CAN WE TAKE CYBER SECURITY FOR GRANTED?

Cyber attacks nowadays can be categorized a severe attack that requires fast response since the attacks cost the world so much. Surprisingly, most of companies are unfortunately lulled into false sense of security for all of this time. The executive management team is usually being overconfident about their company's security because of their cyber security measures such as software solutions, policies and protocols, and routine assessments.

They perceived that cyber security measures alone will be able to tackle the rapid attacks of cyber threats. Even though those measurements looked very promising, companies are not fully secured from crisis inducing error and data breach. Cyber security and digital risk management are not the same; cyber security is a small part integrated with the risk management in order to manage digital risk across an enterprise.

Even though those measurements looked very promising, companies are not fully secured from crisis inducing error and data breach.

As mentioned before, risk management system is a higher and more complex system above the cyber security itself. Despite of its importance, it takes more than cyber security system alone to actually give a decent security shield for your company.

Michael McQueen, the CTO of Criterion, elaborated the comprehensive elements of risk management; there are five crucial pillars that support digital risk management. First pillar is cyber security, which is the set of procedures that regulating system breaches, incident management, and exploit prevention issues. Second pillar is data loss prevention, which is a set of measures in protecting from system failure, corruption, and accidental overwriting and removal. Third pillar is data leakage prevention, which is a set of procedures that preventing users from sending confidential information outside the organizational network. Fourth pillar is availability, which is a set of protections for business processes from disruption due to application downtime. Lastly, fifth pillar is governance, which is a set of policies included obligation, regulation, compliance, client contractual requirements and data custodianship.

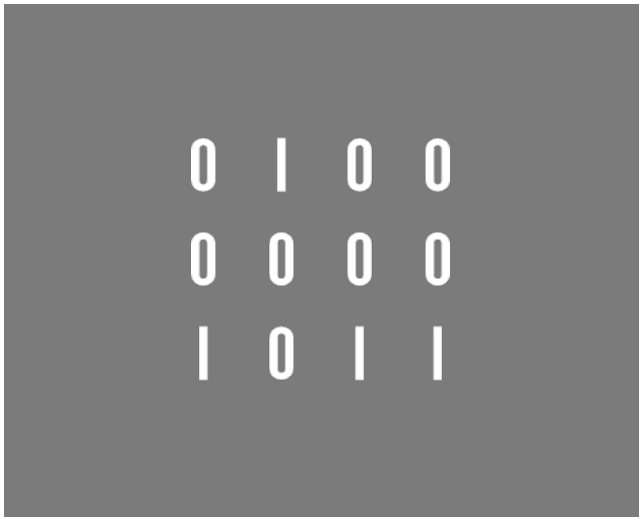
Gartner, an international information technology research and advisory company, conducted an executive survey and the published report told us that approximately 60% of large companies were attacked by cyber breach because their IT security teams failed to manage digital risk with the new technologies, proliferation of connected devices, and the interdependency between these devices.

On the other time, Gartner is also published a report entitled "Top 10 Strategic Predictions for Businesses to watch out for", it said that one-third of large scale companies that relied on digital activities and models probably will hire a digital risk officer in 2017. Also mentioned that by 2018, digital businesses will start open recruiting for about 500% digital jobs and requires less IT business process workers for almost 50%.

This is a very drastic and huge transition in IT staffing across industries, if this is really going to happen, organizations will probably be rushing to recruit candidates to fulfill digital risk positions. In the mean time, IT department staff will lack the required skill set to assess and manage digital risk at both a tactical and strategic level effectively.

Large companies need to prepare themselves for not falling into the 60% majority of companies who suffered from data breach because of their failure in managing digital risk. Firstly, they need to integrate all of the aspects of digital risk management since disintegration can potentially lead into digital crisis.

Companies need to take a lesson from Anthem's breach; sources said that the hackers were using a sophisticated malicious software program when breaking into the Anthem's staff login credentials before finally gained access to the health care provider's network.



The other example is from Target breach; hackers were hijacking the point-of-sale systems and leveraged Target's vendor portal access to take over the retailer's servers. Secondly, companies should make an independent team to provide digital risk transparency assessment.

Data breach occurred mainly because of the combination between human error and poorly designed workflows.

Data breach occurred mainly because of the combination between human error and poorly designed workflows; therefore, an independent review is necessary to provide accurate report around potential risk factors. Lastly, companies need to integrate skillful experts to effectively manage digital risk. To make sure that the company is able to gain the best possible digital risk protection and avoid breach, digital risk management requires highly specialized knowledge of data management and protection practices, defensive architecture for public facing applications, and advanced systems engineering and architecture.

Digital risk management is a complex effort that requires real time monitoring, strategic information architecture, development, operations, data integrations and information systems. Many experts believed that many cases of data breach were able to be prevented if only companies are educated about their vendor's digital risk. Data breach cases also could have been avoided if companies had decent digital risk management strategies and policies in place. Companies should understand if they suffer from data breach. It is their company name and balance sheet that is on stakes.

JUMP START YOU CAREER IN

RISK MANAGEMENT

ENTERPRISE RISK MANAGEMENT

ASSOCIATE PROFESSIONAL

ERMAP or Enterprise RIsk Management Associate Professional is a professional certification issued by ERMA, designed on the ground of ISO 31000 Risk Management International Standard.

ERMAP is given to professionals who are comparatively less experienced in the field of enterprise risk management, but are able to demonstrate an integrated and comprehensive knowledge of the essential principles and fundamental concepts required for managing enterprise-wide risks.

ERMAP
Enterprise Risk Management
ASSOCIATE PROFESSIONAL
ERM ACADEMY

Visit **erm-academy.org/ermap**

HOW SAFE ARE YOUR PASSWORDS?

You think you're secure enough? Think again. Here are the top 25 most used passwords in 2014, recently released by SplashData . If you use any of these, you might want to ditch them immediately.

1. password
2. 1234
3. 123456
4. 12345678
5. 12345
6. 123456789
7. 1234567
8. 123123
9. 696969
10. abc123
11. 111111
12. qwerty
13. baseball
14. dragon
15. football
16. monkey
17. letmein
18. mustang
19. shadow
20. trustno1
21. master
22. access
23. michael
24. superman
25. batman

AUDIT AND CYBER SECURITY

People always relate cyber system to IT or other technical terms, but different approaches have been taken from internal audit departments who are worried about data breach concern. They try to see things from other perspective and they come up with simple yet impressive solution that can save the business; internal audit experts are able to lend a hand and expertise to strengthen cyber security and protection. In fact, if the company is willing to dig deeper into their risk management and assessment, they will find out that such seemingly simple action can do a lot for their performance.

Different experts say different things about how internal audit can do a lot of good things for cyber security, but they all say the similar thing: cyber security can be strengthened, assessed, checked, and monitored through regular and continuous internal audit.

Tom O'Reilly claims that most auditors are intimidated when they run across technical terms like segmented networks, firewall, vulnerability testing, and domains, but if they are able to see past those terms, they will see that those are just...well, terms.

Once the auditors see how familiar the process is, they can perform their work as usual, starting to assess the company's strength and vulnerability, and see the potential holes where the breach may occur.

Being the director for internal audit department at Analog Devices, O'Reilly speaks from experience. He claims that once the auditor is able to break through the technical barrier, they should be able to do a lot for the company's cyber system.

According to David Brand, the man responsible for the IT global audit at Protiviti, the problems about whether the role of internal audit is crucial or not has been around for quite a while. Most people – as well as most departments – have underestimated the role of internal audit, thinking that they know nothing or that cyber security isn't their 'thing'. The fact is that most of internal audit's work is based on process – which can be done by those with good skills and abilities. If the auditors have very thorough and detailed attention to the issues, they can be valuable assets for the company. Once the auditors understand the business itself, the strategy being used, the purpose of the work, the information produced, and what kind of data or information they want to protect, the auditors can start from there.

Richard Chambers even claims that the issue of cyber security isn't exclusive to IT issue alone, but it covers business process too. Being the CEO and President of Institute of Internal Auditors, he has seen similar trends going on. This matter is similar to the previous Y2K issue happening around the end of 1990s.

The same notion is also said by Skip Westfall, Grant Thornton's managing director, stating that cyber security isn't just about IT problem alone. If the company is wise and smart, they should be able to come up with solution of how to address the issue, instead of sit down and do nothing; letting each department works on their own.

Shuaib Shakoor, a partner at Sunera, the outsourcing firm for internal audit, says that companies should start gathering their experts in legal, IT, governance, privacy, internal audit, and also other expertise and areas to come up with a solid plan. If companies are able to do this, they will come with effective holistic scheme, resulting in preventive planning.

The role of internal audit really matters when the company deals with new process, new information, or new product release. Of course, every department is expected to work together in this matter as the plan to secure the system or to strengthen the security won't work well if such plan isn't implemented consistently or rigorously.

Carolyn Holcomb, a partner on cyber security and privacy with PwC claims that such planning is implemented on longer and ongoing terms. Instead of having annual checking or biannual test, the internal audit departments should consider ongoing monitoring and control.

All in all, the role of internal audit is crucial in a company, and it has far expanded beyond the traditional and old school function. In today's global platform, where cyber threats is eminent, internal audit can do a lot – and companies should start considering their part to come up with solid plan and scheme to tackle the emerging cyber threats.

++

ERMA | ENTERPRISE RISK MANAGEMENT ACADEMY

RISKVIEW

(c) 2015, Enterprise Risk Management Academy, ERMA Pte Ltd
All contents featured in RiskView belong to its respective author(s). RISKVIEW Magazine is a quarterly publication on risk management managed and released by ERMA (Enterprise Risk Management Academy).

To find out more about ERMA, visit www.erm-academy.org

CONNECT WITH ERMA
info@erm-academy.org | www.erm-academy.org

@ERMAcademy

erm-academy